NORME INTERNATIONALE

ISO/CEI 10181-7

Première édition
1996-08-01

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Cadres de sécurité pour les systèmes ouverts: Cadre d'audit et d'alarmes de sécurité

Information technology — Open Systems Interconnection — Security frameworks for open systems: Security audit and alarms framework

Numéro de référence
ISO/CEI 10181-7:1996(F)

Sommaire

Version française tirée en 1997

Imprimé en Suisse

Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment ensemble un système consacré à la normalisation internationale considérée comme un tout. Les organismes nationaux membres de l'ISO ou de la CEI participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des différents domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de la CEI collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales ou non gouvernementales, en liaison avec l'ISO et la CEI participent également aux travaux.

Dans le domaine des technologies de l'information, l'ISO et la CEI ont créé un comité technique mixte, l'ISO/CEI JTC 1. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour approbation, avant leur acceptation comme Normes internationales. Les Normes internationales sont approuvées conformément aux procédures qui requièrent l'approbation de 75 % au moins des organismes nationaux votants.

La Norme internationale ISO/CEI 10181-7 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 21, *Interconnexion des systèmes ouverts, gestion des données et traitement distribué ouvert*, en collaboration avec l'UIT-T. Le texte identique est publié en tant que Recommandation UIT-T X.816.

L'ISO/CEI 10181 comprend les parties suivantes, présentées sous le titre général *Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Cadres de sécurité pour les systèmes ouverts*:

— *Partie 1: Présentation*

— *Partie 2: Cadre d'authentification*

— *Partie 3: Cadre de contrôle d'accès*

— *Partie 4: Cadre de non-répudiation*

— *Partie 5: Cadre de confidentialité*

— *Partie 6: Cadre d'intégrité*

— *Partie 7: Cadre d'audit et d'alarmes de sécurité*

Les annexes A à D de la présente partie de l'ISO/CEI 10181 sont données uniquement à titre d'information.

Introduction

La présente Recommandation | Norme internationale précise le concept d'audit de sécurité défini dans la Rec. UIT-T X.810 | ISO/CEI 10181-1. Cela comprend la détection d'événements ainsi que les actions résultantes de ces événements. Le cadre couvre donc à la fois l'audit de sécurité et les alarmes de sécurité.

Un audit de sécurité est une analyse et un examen – effectués de façon indépendante – des enregistrements et activités du système. Les objectifs d'un audit de sécurité sont les suivants:

- aider à l'identification et l'analyse d'actions non autorisées ou d'attaques;
- aider à garantir que les actions peuvent être attribuées aux entités responsables de ces actions;
- contribuer au développement de procédures améliorées de contrôle des dommages;
- confirmer la conformité avec la politique de sécurité établie;
- signaler l'information qui peut indiquer des inadéquations dans le contrôle du système;
- identifier les changements possibles requis dans les contrôles, la politique et les procédures.

Dans ce cadre, un audit de sécurité consiste en la détection, la collecte et l'enregistrement des événements liés à la sécurité des systèmes ouverts dans un journal d'audit de sécurité et en l'analyse de ces événements.

L'audit mais aussi l'imputabilité nécessitent le stockage de l'information. Un audit de sécurité garantit que l'information enregistrée concerne à la fois les événements routiniers et les événements exceptionnels, de sorte que des investigations ultérieures puissent déterminer si des violations de sécurité sont survenues et, si tel est le cas, quelles sont les informations ou les autres ressources qui ont été compromises. L'imputabilité garantit que l'information relative aux actions réalisées par les utilisateurs, ou par des processus agissant pour leur compte, est enregistrée, de telle sorte que les conséquences de ces actions puissent être ultérieurement liées aux utilisateurs en question et que les utilisateurs puissent être tenus responsables de ces actions. La fourniture d'un service d'audit de sécurité peut contribuer à assurer l'imputabilité.

Une alarme de sécurité est une indication émise vers un individu ou un processus pour indiquer qu'une situation pouvant nécessiter une action à temps est apparue. Les objectifs d'un service d'alarme de sécurité sont les suivants:

- signaler des tentatives réelles ou apparentes de violer la sécurité;
- signaler divers événements liés à la sécurité, y compris les événements «normaux»;
- signaler les événements déclenchés par l'atteinte des limites de seuil.

NORME INTERNATIONALE

RECOMMANDATION UIT-T

TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DE SYSTÈMES OUVERTS (OSI) – CADRES DE SÉCURITÉ POUR LES SYSTÈMES OUVERTS: CADRE D'AUDIT ET D'ALARMES DE SÉCURITÉ

1 Domaine d'application

La présente Recommandation | Norme internationale couvre l'application des services de sécurité dans un environnement de systèmes ouverts, où le terme «systèmes ouverts» est utilisé pour des domaines tels que les bases de données, les applications distribuées, le traitement ODP et l'interconnexion OSI. Les cadres de sécurité sont destinés à définir les moyens d'offrir la protection pour les systèmes et les objets au sein des systèmes, ainsi que les interactions entre systèmes. Les cadres ne couvrent pas la méthodologie de construction des systèmes ou mécanismes.

Les cadres couvrent à la fois les éléments de données et les séquences d'opérations (mais pas les éléments de protocole) utilisés pour obtenir des services spécifiques de sécurité. Ces services de sécurité peuvent s'appliquer aux entités communicantes des systèmes aussi bien qu'aux données échangées entre systèmes, ainsi qu'aux données gérées par les systèmes.

Le but de l'audit et des alarmes de sécurité décrits dans la présente Recommandation | Norme internationale est d'assurer que les événements liés à la sécurité des systèmes ouverts sont manipulés en accord avec la politique de sécurité de l'autorité de sécurité en vigueur.

En particulier, ce cadre de sécurité:

a) définit les concepts élémentaires d'audit et d'alarmes de sécurité;

b) fournit un modèle général pour l'audit et les alarmes de sécurité;

c) identifie les relations du service d'audit et d'alarmes de sécurité avec d'autres services de sécurité.

Comme les autre services de sécurité, un audit de sécurité ne peut être fourni que dans le contexte d'une politique de sécurité définie.

Le modèle d'audit et d'alarmes de sécurité indiqué dans l'article 6 de ce cadre répond à une variété d'objectifs qui peuvent ne pas être tous nécessaires ou souhaités dans un environnement particulier. Le service d'audit de sécurité offre à une autorité d'audit la possibilité de spécifier les événements qui doivent être enregistrés dans un journal d'audit de sécurité.

Plusieurs types de normes différents peuvent utiliser ce cadre, y compris:

1) les normes qui incorporent le concept d'audit et d'alarmes;

2) les normes qui spécifient des services abstraits comprenant l'audit et les alarmes;

3) les normes qui spécifient les utilisations d'audit et d'alarmes;

4) les normes qui spécifient les moyens de fournir l'audit et les alarmes au sein d'une architecture de système ouvert;

5) les normes qui spécifient les mécanismes d'audit et d'alarmes.

De telles normes peuvent utiliser ce cadre de la façon suivante:

– les normes de types 1), 2), 3), 4) et 5) peuvent utiliser la terminologie de ce cadre;

– les normes de types 2), 3), 4) et 5) peuvent utiliser les fonctionnalités définies dans l'article 8 de ce cadre;

– les normes de type 5) peuvent être basées sur les caractéristiques des mécanismes définis dans l'article 9 de ce cadre.

2 Références normatives

Les Recommandations et Normes internationales suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Recommandation | Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute Recommandation et Norme sont sujettes à révision et les parties prenantes aux accords fondés sur la présente Recommandation | Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et Normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur. Le Bureau de la normalisation des télécommunications de l'UIT tient à jour une liste des Recommandations de l'UIT-T en vigueur.

2.1 Recommandations | Normes internationales identiques

- Recommandation UIT-T X.200 (1994) | Norme ISO/CEI 7498-1:1994, *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de référence de base: le modèle de référence de base.*
- Recommandation X.734 du CCITT (1992) | ISO/CEI 10164-5:1993, *Technologies de l'information – Interconnexion des systèmes ouverts – Gestion-systèmes: fonction de gestion des rapports d'événement.*
- Recommandation X.735 du CCITT (1992) | ISO/CEI 10164-6:1993, *Technologies de l'information – Interconnexion des systèmes ouverts – Gestion-systèmes: fonction de commande des registres de consignation.*
- Recommandation X.736 du CCITT (1992) | ISO/CEI 10164-7:1992, *Technologies de l'information – Interconnexion des systèmes ouverts – Gestion-systèmes: fonction de signalisation des alarmes de sécurité.*
- Recommandation X.740 du CCITT (1992) | ISO/CEI 10164-8:1993, *Technologies de l'information – Interconnexion des systèmes ouverts – Gestion-systèmes: fonction de piste de vérification de sécurité.*
- Recommandation UIT-T X.810 (1995) | ISO/CEI 10181-1:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: aperçu général.*

2.2 Paires de Recommandations | Normes internationales équivalentes par leur contenu technique

- Recommandation X.700 du CCITT (1992), *Cadre de gestion pour l'interconnexion de systèmes ouverts pour les applications du CCITT.*

  ISO/CEI 7498-4:1989, *Systèmes de traitement de l'information – Interconnexion des systèmes ouverts – Modèle de référence de base – Partie 4: Cadre général de gestion.*
- Recommandation X.800 du CCITT (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT.*

  ISO 7498-2:1989, *Systèmes de traitement de l'information – Interconnexion des systèmes ouverts – Modèle de référence de base – Partie 2: Architecture de sécurité.*

3 Définitions

Pour les besoins de la présente Recommandation | Norme internationale, les définitions suivantes s'appliquent.

3.1 Définitions du modèle de référence de base

La présente Recommandation | Norme internationale utilise les termes suivants définis dans la Rec. UIT-T X.200 | ISO/CEI 7498-1:

a) entité;

b) fonctionnalité;

c) fonction;

d) service.

3.2 Définitions de l'architecture de sécurité

La présente Recommandation | Norme internationale utilise les termes suivants définis dans la Rec. X.800 du CCITT | ISO/CEI 7498-2:

a) imputabilité;

b) disponibilité;

c) audit de sécurité;

d) journal d'audit de sécurité;

e) politique de sécurité.

3.3 Définitions du cadre de gestion

La présente Recommandation | Norme internationale utilise le terme suivant défini dans la Rec. X.700 du CCITT | ISO/CEI 7498-4:

– objet géré.

3.4 Définitions de l'aperçu général du cadre de sécurité

La présente Recommandation | Norme internationale utilise le terme suivant défini dans la Rec. UIT-T X.810 | ISO/CEI 10181-1:

– domaine de sécurité.

3.5 Définitions additionnelles

Pour les besoins de la présente Recommandation | Norme internationale, les définitions suivantes s'appliquent.

3.5.1 processeur d'alarme: fonction qui, en réponse à une alarme de sécurité, génère une action appropriée et génère un message d'audit de sécurité.

3.5.2 autorité d'audit: gestionnaire responsable de la définition des aspects d'une politique de sécurité applicables à la conduite d'un audit de sécurité.

3.5.3 analyseur d'audit: fonction qui vérifie un journal d'audit de sécurité afin de produire, si cela est approprié, des messages d'alarme de sécurité et des messages d'audit de sécurité.

3.5.4 archiviste d'audit: fonction qui archive une partie du journal d'audit de sécurité.

3.5.5 expéditeur d'audit: fonction qui transfère, à la fonction de collecte de journal de sécurité, des parties ou la totalité d'un journal distribué d'audit de sécurité.

3.5.6 examinateur de journal d'audit: fonction qui, à partir d'un ou plusieurs journaux d'audit de sécurité, construit des rapports.

3.5.7 enregistreur d'audit: fonction qui génère des enregistrements d'audit de sécurité et les stocke dans un journal d'audit de sécurité.

3.5.8 fournisseur d'audit: fonction qui fournit des enregistrements de journal d'audit de sécurité en fonction de certains critères.

3.5.9 collecteur de journal d'audit: fonction qui rassemble les enregistrements d'un journal distribué d'audit dans un journal d'audit de sécurité.

3.5.10 filtre d'événement: fonction qui fournit une analyse initiale des événements liés à la sécurité et génère un message d'audit de sécurité et/ou un message d'alarme.

3.5.11 alarme de sécurité: message généré lorsqu'un événement lié à la sécurité, défini par la politique de sécurité comme étant une condition d'alarme, a été détecté. Une alarme de sécurité est destinée à être portée à temps à l'attention d'entités appropriées.

3.5.12 **administrateur d'alarme de sécurité**: individu ou processus qui détermine la nature des alarmes de sécurité.

3.5.13 **événement lié à la sécurité**: tout événement qui a été défini par la politique de sécurité comme une brèche potentielle dans la politique de sécurité, ou comme ayant un intérêt potentiel pour la sécurité. L'arrivée à une valeur prédéfinie de seuil est un exemple d'événement lié à la sécurité.

3.5.14 **message d'audit de sécurité**: message généré à la suite d'un événement vérifiable lié à la sécurité.

3.5.15 **enregistrement d'audit de sécurité**: enregistrement unique dans un journal d'audit de sécurité.

3.5.16 **agent d'audit de sécurité**: individu ou processus autorisé à avoir accès au journal de sécurité et à bâtir des rapports d'audit.

3.5.17 **rapport de sécurité**: rapport qui résulte d'une analyse du journal d'audit de sécurité et qui peut être utilisé pour déterminer si une brèche est apparue dans la sécurité.

4 Abréviations

OSI Interconnexion des systèmes ouverts (*open systems interconnection*).

5 Notation

Sauf indication contraire, les termes «service» et «mécanisme» sont utilisés pour désigner, respectivement, le «service d'audit de sécurité» et le «mécanisme d'audit de sécurité»; celui d'«audit» désigne un «audit de sécurité» et enfin, celui d'«alarme» désigne une «alarme de sécurité».

6 Présentation générale de l'audit et des alarmes de sécurité

Cet article décrit un modèle permettant de manipuler les alarmes de sécurité et de conduire un audit de sécurité pour les systèmes ouverts.

Un audit de sécurité permet d'évaluer l'adéquation de la politique de sécurité, d'aider à la détection des violations de sécurité, de faciliter l'imputation de leurs actions aux individus (ou des actions des entités agissant pour leur compte), d'aider à la détection de mauvaise utilisation des ressources, et agit comme élément préventif pour les individus qui pourraient tenter d'endommager le système. Les mécanismes d'audit de sécurité ne sont pas directement mis en jeu dans la prévention des violations de sécurité: ils sont impliqués pour la détection, l'enregistrement et l'analyse des événements. Cela permet de mettre en œuvre des changements dans les procédures opérationnelles en réponse à des événements anormaux comme des violations de sécurité.

Une alarme de sécurité est générée suite à la détection de tout événement lié à la sécurité qui a été défini par la politique de sécurité comme étant une condition d'alarme. Cela pourrait inclure le cas de l'obtention d'un seuil prédéfini. Certains de ces événements peuvent nécessiter une action immédiate alors que d'autres peuvent nécessiter une investigation plus poussée pour déterminer si une action est requise.

Une mise en œuvre du modèle d'audit et d'alarmes de sécurité peut nécessiter l'utilisation d'autres services de sécurité pour réaliser le service d'audit et d'alarmes de sécurité et pour assurer son fonctionnement correct et sûr. Ce sujet est abordé plus loin dans l'article 10.

Bien que l'utilisation des journaux d'audit de sécurité et d'audits de sécurité ait des caractéristiques spéciales, d'autres journaux d'audit et d'autres audits (autres que de sécurité) peuvent recourir aux fonctions et mécanismes décrits dans le présent cadre.

Comme avec les autres aspects de la sécurité, on obtient une efficacité maximale en s'assurant que les besoins spécifiques d'audit de sécurité sont conçus dans le système. Les concepteurs de système devraient donc tenir compte du besoin de vérifier (par exemple, examen et analyse tout prêts) à la fois le processus de conception et le système en cours de développement.

NOTE – Le modèle d'audit et d'alarmes de sécurité n'indique pas comment les autres systèmes de gestion et les caractéristiques opérationnelles sont liés à ce modèle.

6.1 Modèle et fonctions

Le modèle présenté ci-dessous illustre les fonctions utilisées dans la fourniture du service d'audit et d'alarmes de sécurité.

6.1.1 Fonctions du service d'audit et d'alarmes de sécurité

Diverses fonctions sont nécessaires pour mettre en œuvre un service complet d'audit et d'alarmes de sécurité, à savoir:

- le **filtre d'événement** qui fournit une analyse initiale de l'événement et détermine s'il envoie l'événement à l'enregistreur d'audit ou au processeur d'alarme;
- l'**enregistreur d'audit** qui génère les enregistrements d'audit à partir des messages reçus et stocke les enregistrements dans un journal d'audit de sécurité;
- le **processeur d'alarme** qui génère à la fois un message d'audit et une action appropriée en réponse à une alarme de sécurité;
- l'**analyseur d'audit** qui vérifie un journal d'audit de sécurité et, si cela est approprié, produit des messages d'alarme et des messages d'audit de sécurité;
- l'**examinateur de journal d'audit** qui bâtit des rapports de sécurité à partir d'un ou de plusieurs journaux d'audit de sécurité;
- le **fournisseur d'audit** qui fournit des enregistrements d'audit de sécurité en fonction de certains critères;
- l'**archiviste d'audit** qui archive une partie du journal d'audit de sécurité.

Des fonctions supplémentaires peuvent s'avérer nécessaires pour mettre en œuvre des journaux d'audit de sécurité distribués et des alarmes. Parmi celles-ci:

- la fonction de **collecteur de journal d'audit** qui rassemble les enregistrements d'un journal distribué d'audit dans un journal d'audit de sécurité;
- la fonction d'**expéditeur d'audit** qui transfère, à la fonction de collecte de journal de sécurité, des parties ou la totalité d'un journal distribué d'audit de sécurité.

6.1.2 Modèle d'audit et d'alarmes de sécurité

Le modèle d'audit et d'alarmes de sécurité décrit ci-dessous fait intervenir plusieurs phases. Suite à la détection d'un événement, la détermination de son intérêt ou non pour la sécurité doit être effectuée. Le *filtre d'événement* évalue l'événement pour déterminer si un message d'audit de sécurité et/ou un message d'alarme de sécurité devrait être généré. Les messages d'audit de sécurité sont envoyés à l'*enregistreur d'audit*: les alarmes de sécurité sont envoyées au *processeur d'alarme* pour évaluation et action ultérieure. Les messages d'audit de sécurité sont alors formatés puis transformés en enregistrements d'audit de sécurité pour être consignés dans le journal d'audit de sécurité. Les anciennes parties du journal d'audit de sécurité peuvent être archivées et le journal d'audit de sécurité ainsi que les archives de journal d'audit de sécurité peuvent être utilisés pour bâtir des rapports d'audit en sélectionnant, en fonction de critères spécifiés, des enregistrements particuliers d'audit de sécurité. C'est ainsi que le journal d'audit de sécurité peut être analysé et que des rapports et/ou des alarmes de sécurité peuvent être générés. Le modèle d'audit et d'alarmes de sécurité est indiqué sur la Figure 1.

6.1.3 Groupement des fonctions d'audit et d'alarmes de sécurité

Les fonctions décrites dans le modèle peuvent être colocalisées dans un composant d'un système ou distribuées sur plusieurs composants du système. Ces fonctions peuvent également être localisées dans des systèmes d'extrémité différents et peuvent être dupliquées. Dans certains cas, comme pour des raisons de performances, il sera avantageux de grouper ces fonctions. En particulier, un *enregistreur d'audit,* un *expéditeur d'audit*, un *fournisseur d'audit* et un *analyseur d'audit* travaillant ensemble sur le même journal d'audit de sécurité peuvent constituer une partie d'un seul système d'extrémité.

Un autre groupement pourrait être constitué d'un *examinateur de journal d'audit* et d'un *analyseur d'audit* qui peuvent être utiles à un auditeur de sécurité.

Il peut y avoir une chaîne de fonctions arrangées de façon hiérarchique, en particulier dans un journal d'audit de sécurité distribué (voir la Figure 2). Ici un *collecteur de journal d'audit* d'un composant collecte les messages d'audit de l'*expéditeur d'audit* d'un autre composant. La chaîne se termine lorsqu'un composant ne met pas en œuvre un *expéditeur d'audit*: dans ce cas, le composant doit mettre en œuvre un *archiviste d'audit* pour être en mesure d'archiver son journal d'audit de sécurité.

La décision des fonctions, s'il y en a, devant être groupées, est un problème de mise en œuvre. Les exemples ci-dessus ne sont donnés qu'à titre d'exemple.

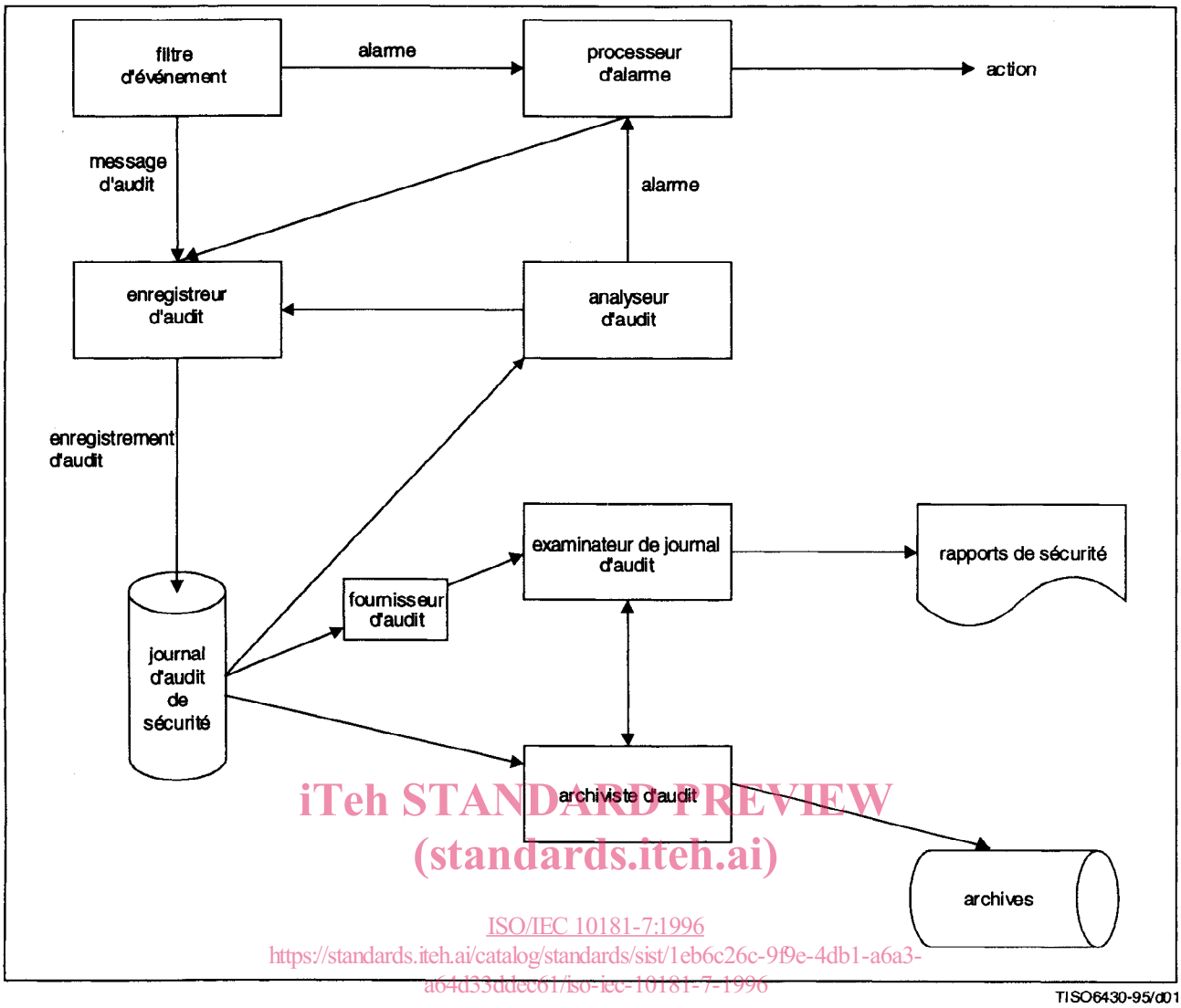

Figure 1 – Modèle d'audit et d'alarmes de sécurité

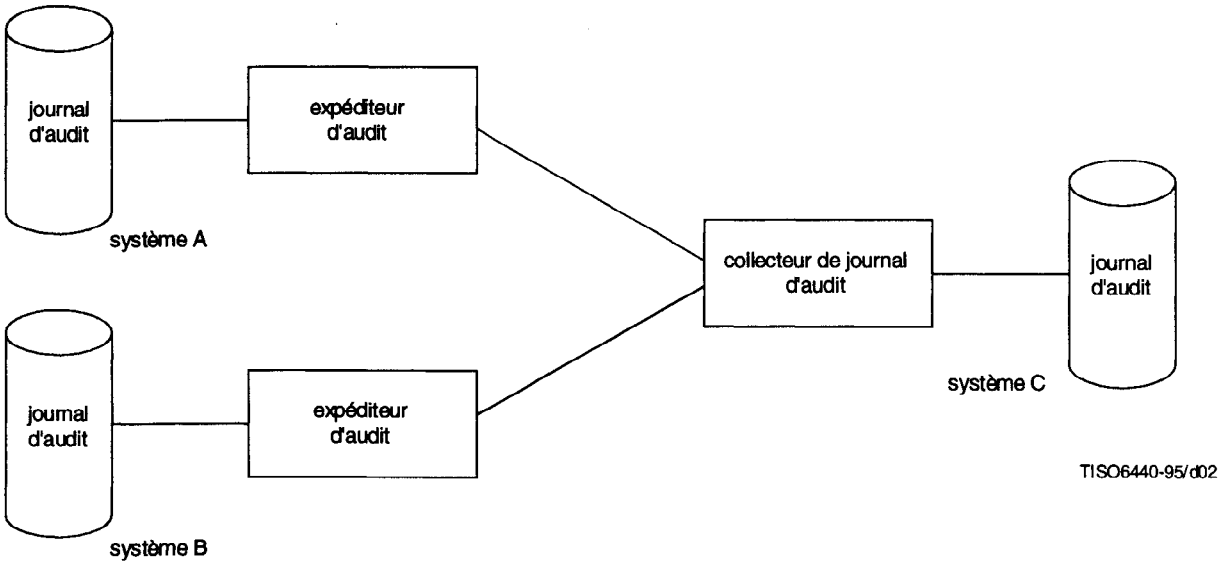

Figure 2 – Modèle de journal d'audit distribué

6.2 Phases des procédures d'audit et d'alarmes de sécurité

Le service d'audit de sécurité fournit à une autorité d'audit la possibilité de spécifier et de sélectionner les événements qui doivent être détectés et enregistrés dans un journal d'audit de sécurité, et les événements qui nécessitent le déclenchement d'une alarme de sécurité et d'un message d'audit de sécurité.

Les phases suivantes peuvent intervenir dans les procédures d'audit:

- phase de détection, dans laquelle un événement lié à la sécurité est détecté;
- phase de filtrage, dans laquelle une détermination initiale est effectuée sur la nécessité d'enregistrer l'événement dans un journal d'audit de sécurité ou d'envoyer une alarme;
- phase de traitement d'alarme, dans laquelle une alarme de sécurité ou un message d'audit de sécurité peut être émis;
- phase d'analyse, dans laquelle un événement lié à la sécurité est évalué avec l'ensemble, et dans le contexte, des éléments précédemment détectés et enregistrés dans le journal d'audit, et une ligne de conduite déterminée;
- phase d'agrégation, dans laquelle des enregistrements de journal d'audit de sécurité distribué sont collectés dans un seul système de journal d'audit de sécurité;
- phase de génération de rapport d'événement, dans laquelle des rapports d'audit de sécurité sont bâtis à partir des enregistrements de journal d'audit de sécurité;
- phase d'archivage, dans laquelle des enregistrements du journal d'audit de sécurité sont transférés dans l'archive de journal d'audit de sécurité.

Les phases décrites ici ne sont pas nécessairement concomitantes dans le temps; elles peuvent, par exemple, se recouvrir.

6.2.1 Phase de détection

La phase de détection met en jeu la détermination de l'apparition d'un événement pouvant être lié à la sécurité. La détermination concrète de l'action, s'il y en a une, devant être prise en réponse à cet événement est la tâche du *filtre d'événement* (voir 6.2.2) mais, dans certains cas, déterminée par la politique de sécurité, une action immédiate peut être initiée.

6.2.2 Phase de filtrage

Lorsqu'un événement lié à la sécurité a été détecté, le filtre d'événement déterminera la ligne de conduite initiale appropriée. L'action sera l'une des suivantes:

a) ne pas prendre d'action;

b) générer un message d'audit de sécurité;

c) générer à la fois une alarme de sécurité et un message d'audit de sécurité.

La décision relative à la ligne de conduite qui devrait être suivie pour chaque événement dépend de la politique de sécurité en vigueur.

6.2.3 Phase de traitement d'alarme

Le processeur de sécurité analyse l'alarme pour déterminer la ligne de conduite adéquate. L'action sera l'une des suivantes:

a) ne pas prendre d'action;

b) initier une action de récupération;

c) initier une action de récupération et générer un message d'audit de sécurité.

La décision de la ligne de conduite qui devrait être suivie pour chaque événement dépend de la politique de sécurité en vigueur.

NOTE – b) et c) pourraient impliquer que l'événement soit porté à l'attention d'une personne comme un responsable de sécurité ou un administrateur d'audit.