NORME INTERNATIONALE

ISO/IEC 27042

Première édition
2015-06-15

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'analyse et l'interprétation des preuves numériques

Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence

Numéro de référence
ISO/IEC 27042:2015(F)

DOCUMENT PROTÉGÉ PAR COPYRIGHT

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Sommaire

Page

Avant-propos ..... **iv**
Introduction ..... **v**
1 Domaine d'application **1**
2 Références normatives **1**
3 Termes et définitions **1**
4 Symboles et abréviations **5**
5 Investigation **5**
5.1 Vue d'ensemble 5
5.2 Continuité 5
5.3 Répétabilité et reproductibilité 5
5.4 Approche structurée 5
5.5 Incertitude 7
6 Analyse **7**
6.1 Vue d'ensemble 7
6.2 Principes généraux 7
6.3 Utilisation des outils 8
6.4 Conservation des archives 8
7 Modèles analytiques **8**
7.1 Analyse statique 8
7.2 Analyse dynamique 9
7.2.1 Vue d'ensemble 9
7.2.2 Analyse dynamique de systèmes dont il ne peut être réalisé d'images ou de copies 9
7.2.3 Analyse dynamique de systèmes dont il peut être réalisé des images ou des copies 9
8 Interprétation **10**
8.1 Généralités 10
8.2 Accréditation des faits 10
8.3 Facteurs affectant l'interprétation 10
9 Consignation **11**
9.1 Préparation 11
9.2 Contenus de rapport suggérés 11
10 Compétence **12**
10.1 Vue d'ensemble 12
10.2 Démonstration de la compétence 12
10.3 Consignation de la compétence 12
11 Aptitude **13**
11.1 Vue d'ensemble 13
11.2 Mécanismes de démonstration de l'aptitude 13
Annexe A (informative) **Exemples de spécifications relatives à la compétence et l'aptitude** **14**
Bibliographie **15**

Avant-propos

L'ISO (Organisation internationale de normalisation) et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de l'IEC participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de l'IEC collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et l'IEC, participent également aux travaux. Dans le domaine des technologies de l'information, l'ISO et l'IEC ont créé un comité technique mixte, l'ISO/IEC JTC 1.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir le lien suivant: www.iso.org/iso/fr/foreword.html.

Le comité responsable de ce document est l'ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité*.

Introduction

Généralités

La présente Norme internationale fournit des préconisations concernant la réalisation de l'analyse et de l'interprétation de preuves numériques éventuelles afin d'identifier et d'évaluer les preuves numériques qui peuvent être utilisées pour comprendre un incident. La nature exacte des données et des informations composant les preuves numériques éventuelles dépendra de la nature de l'incident et des sources de preuves numériques impliquées dans cet incident.

Lors de l'utilisation de la présente Norme internationale, l'utilisateur prend pour hypothèse que les préconisations fournies dans l'ISO/IEC 27035-2 et l'ISO/IEC 27037:2012 ont été suivies et que tous les processus utilisés sont compatibles avec les préconisations de l'ISO/IEC 27043:2015 et de l'ISO/IEC 27041[1)].

Relation avec d'autres normes

La présente Norme internationale est destinée à compléter d'autres normes et documents donnant des préconisations concernant l'investigation, et la préparation à l'investigation, sur des incidents de sécurité de l'information. Elle ne constitue pas un guide exhaustif, mais édicte certains principes fondamentaux visant à garantir que les outils, les techniques et les méthodes soient choisis de manière appropriée et que leur adéquation avec l'application visée puisse être démontrée, le cas échéant.

La présente Norme internationale vise également à informer les décideurs devant déterminer la fiabilité des preuves numériques qui leur sont soumises. Elle s'applique aux organismes devant protéger, analyser et présenter des preuves numériques éventuelles. Elle est pertinente dans le contexte des organismes en charge de l'établissement de politiques, qui créent et évaluent des modes opératoires en rapport avec les preuves numériques, souvent dans le cadre d'un ensemble plus vaste de preuves.

La présente Norme internationale décrit une partie d'un processus d'investigation complet, portant sans s'y limiter sur les thématiques suivantes:

— gestion des incidents, comprenant la préparation et la planification des investigations;

— traitement des preuves numériques;

— utilisation de l'expurgation et problèmes en découlant;

— systèmes de prévention et de détection des intrusions, comprenant les informations pouvant être obtenues à partir de ces systèmes;

— sécurité du stockage, comprenant le nettoyage du stockage;

— vérification de l'adéquation avec l'application visée des méthodes d'investigation;

— analyse et interprétation des preuves numériques;

— connaissance des principes et processus liés à l'investigation des preuves numériques;

— gestion des événements d'incident de sécurité, comprenant l'établissement de preuve à partir de systèmes impliqués dans la gestion des événements d'incident de sécurité;

— relation entre la découverte électronique et les autres méthodes d'investigation, et utilisation des techniques de découverte électronique dans d'autres investigations;

— gouvernance des investigations, comprenant les investigations forensiques.

Ces thématiques sont couvertes partiellement dans les normes ISO/IEC suivantes:

— ISO/IEC 27037;

1) Publication en attente

La présente Norme internationale décrit les moyens par lesquels les personnes impliquées dans les premières phases d'une investigation, comprenant la réponse initiale, peuvent s'assurer que des preuves numériques éventuelles suffisantes sont recueillies pour permettre de poursuivre l'investigation de manière appropriée.

— ISO/IEC 27038;

Certains documents peuvent contenir des informations dont il ne faut pas qu'elles soient divulguées auprès de certaines communautés. Des documents modifiés peuvent être diffusés auprès de ces communautés, après un traitement approprié du document d'origine. Le processus consistant à supprimer les informations à ne pas divulguer est intitulé l'«expurgation».

L'expurgation numérique des documents est un domaine relativement récent des pratiques de gestion documentaire, qui soulève des problèmes spécifiques et pose des risques potentiels. Lors de l'expurgation de documents numériques, il faut que les informations supprimées ne soient pas récupérables. Dès lors, il est nécessaire de prendre des précautions pour que les informations expurgées soient supprimées définitivement du document numérique (par exemple il ne faut pas qu'elles soient simplement masquées dans des parties non affichables du document).

La norme ISO/IEC 27038 spécifie les méthodes d'expurgation numérique de documents numériques. Elle spécifie également les exigences concernant les logiciels utilisables pour l'expurgation.

— ISO/IEC 27040:2015;

La présente Norme internationale donne des préconisations techniques détaillées concernant la manière dont les organismes peuvent définir un niveau approprié d'atténuation du risque grâce à l'emploi d'une approche reconnue et cohérente de la planification, la conception, la documentation et la mise en œuvre de la sécurité de stockage des données. La sécurité du stockage s'applique à la protection (la sécurité) des informations là où elles sont stockées et à la sécurité des informations transférées au moyen des liaisons de communication associées au stockage. La sécurité du stockage comprend la sécurité des dispositifs et des supports, la sécurité des activités de management associées aux dispositifs et aux supports, la sécurité des applications et des services et la sécurité relative aux utilisateurs finaux pendant la durée de vie de leurs dispositifs et supports et après la fin de leur utilisation.

Les mécanismes de sécurité tels que le chiffrement et le nettoyage peuvent affecter la capacité d'investigation d'une personne en mettant en place des mécanismes d'obfuscation. Ils doivent être pris en compte en amont et au cours d'une investigation. Ils peuvent également être importants pour s'assurer que le stockage des matériaux probatoires, au cours et en aval d'une investigation, soit préparé et sécurisé de manière adéquate.

— ISO/IEC 27041;

Il est important de pouvoir démontrer que les méthodes et processus déployés au cours d'une investigation sont appropriés. La présente Norme internationale fournit des préconisations concernant la façon de s'assurer que des méthodes et processus satisfont aux exigences de l'investigation et ont été soumises à essai de façon appropriée.

— ISO/IEC 27043:2015;

La présente Norme internationale définit les grands principes et processus communs sous-jacents à une investigation sur incident, et fournit un modèle cadre pour toutes les phases des investigations.

Les projets ISO/IEC suivants couvrent également en partie les thématiques identifiées ci-dessus et peuvent conduire à la publication de normes pertinentes, suite à la publication de la présente Norme internationale.

— ISO/IEC 27035 (toutes les parties);

Cette norme en trois parties fournit aux organismes une approche structurée et planifiée de la gestion des incidents de sécurité. Elle se compose des parties suivantes.

— ISO/IEC 27035-1;

Cette partie présente les concepts de base et les phases de la gestion des incidents de sécurité de l'information. Elle combine ces concepts à des principes selon une approche structurée de détection, consignation, évaluation, réponse et application des enseignements tirés.

— ISO/IEC 27035-2;

Cette partie présente les concepts à planifier et à préparer dans le cadre de la réponse aux incidents. Ces concepts, comprenant la politique et le plan de gestion des incidents, la constitution de l'équipe de réponse aux incidents, et les réunions d'information et la formation de sensibilisation, sont basés sur la phase de planification et de préparation du modèle présenté dans l'ISO/IEC 27035-1. Cette partie couvre également la phase du modèle intitulée «Enseignements tirés».

— ISO/IEC 27035-3;

Cette partie couvre les responsabilités du personnel et les activités pratiques de réponse aux incidents pour l'ensemble de l'organisme. Une attention particulière est accordée aux activités de l'équipe de réponse aux incidents, comprenant les activités de surveillance, de détection, d'analyse et de réponse menées sur les données recueillies ou les événements de sécurité.

— ISO/IEC 27044[2)];

Elle fournit des lignes directrices aux organismes concernant la préparation du déploiement des informations de sécurité et des processus/systèmes de gestion des événements. Elle traite notamment de la sélection, du déploiement et des opérations de gestion d'évènements et d'informations de sécurité (SIEM). Elle vise spécifiquement à offrir une assistance pour satisfaire aux exigences de l'ISO/IEC 27001 concernant la mise en œuvre de modes opératoires et d'autres contrôles en mesure de permettre une détection et une réponse rapides aux incidents de sécurité, pour exécuter un contrôle et des modes opératoires de revue en vue d'identifier de façon adéquate les violations et incidents de sécurité avortés et réussis.

— ISO/IEC 27050 (toutes les parties)[3)];

Ce projet couvre les activités liées à la découverte électronique, comprenant sans s'y limiter l'identification, la préservation, la collecte, le traitement, la revue, l'analyse et la production de stockage électronique d'informations (ESI). Il fournit en outre des préconisations concernant les mesures, allant de la création initiale d'ESI à leur élimination finale, qu'un organisme peut prendre pour atténuer les risques et réduire les dépenses, s'il s'avère que la découverte électronique devient problématique. Il concerne à la fois les membres du personnel associés à des fonctions techniques et non techniques, impliqués dans tout ou partie des activités de découverte électronique. Il est important de noter que ces préconisations ne se destinent pas à contredire ou se substituer aux législations et réglementations locales.

La découverte électronique constitue souvent un vecteur pour les investigations, ainsi que les activités d'acquisition et de traitement de preuves. En outre, la sensibilité et la criticité des données nécessitent parfois des protections telles que la sécurité du stockage, pour se prémunir contre les violations de données.

— ISO/IEC 30121:2015;

La présente Norme internationale fournit un cadre pour les organes de gouvernance des organismes (comprenant les propriétaires, les membres du conseil d'administration, les directeurs, les partenaires, les cadres dirigeants ou des fonctions similaires), sur la meilleure façon de préparer un organisme aux investigations numériques avant leur occurrence. La présente Norme internationale s'applique au développement de processus (et de décisions) stratégiques concernant la conservation, la disponibilité, l'accès et l'efficience économique de la divulgation de preuves numériques. Elle s'applique aux organismes de tous types et de toutes tailles. Elle concerne la préparation stratégique avisée d'un organisme à l'investigation numérique. La préparation à l'approche forensique garantit qu'un organisme a engagé

2) Publication en attente

3) Publication en attente

une préparation stratégique appropriée et pertinente pour donner son aval concernant des événements potentiels de nature probatoire. Des actions peuvent se produire suite à d'inévitables violations de sécurité, fraudes et revendications quant à la réputation. Dans chaque situation, les technologies de l'information (TI) doivent être déployées de manière stratégique afin d'optimiser la disponibilité des preuves, leur accessibilité et leur efficience économique.

La Figure 1 représente les activités types liées à un incident et à l'investigation s'y rapportant. Les références représentées dans la figure (par exemple 27037) désignent les Normes internationales répertoriées ci-dessus; les barres grisées représentent les classes/activités auxquelles chacune d'elles est la plus susceptible d'être directement applicable ou sur lesquelles chacune d'elles exerce une certaine influence sur le processus d'investigation (par exemple en stipulant une politique ou en instaurant des contraintes). Il convient cependant qu'elles soient toutes consultées en amont et au cours des phases de planification et de préparation. Les classes de processus qui sont représentées font l'objet d'une définition complète dans cette Norme internationale et les activités identifiées correspondent à celles évoquées plus en détail dans l'ISO/IEC 27035-2 et l'ISO/IEC 27037.

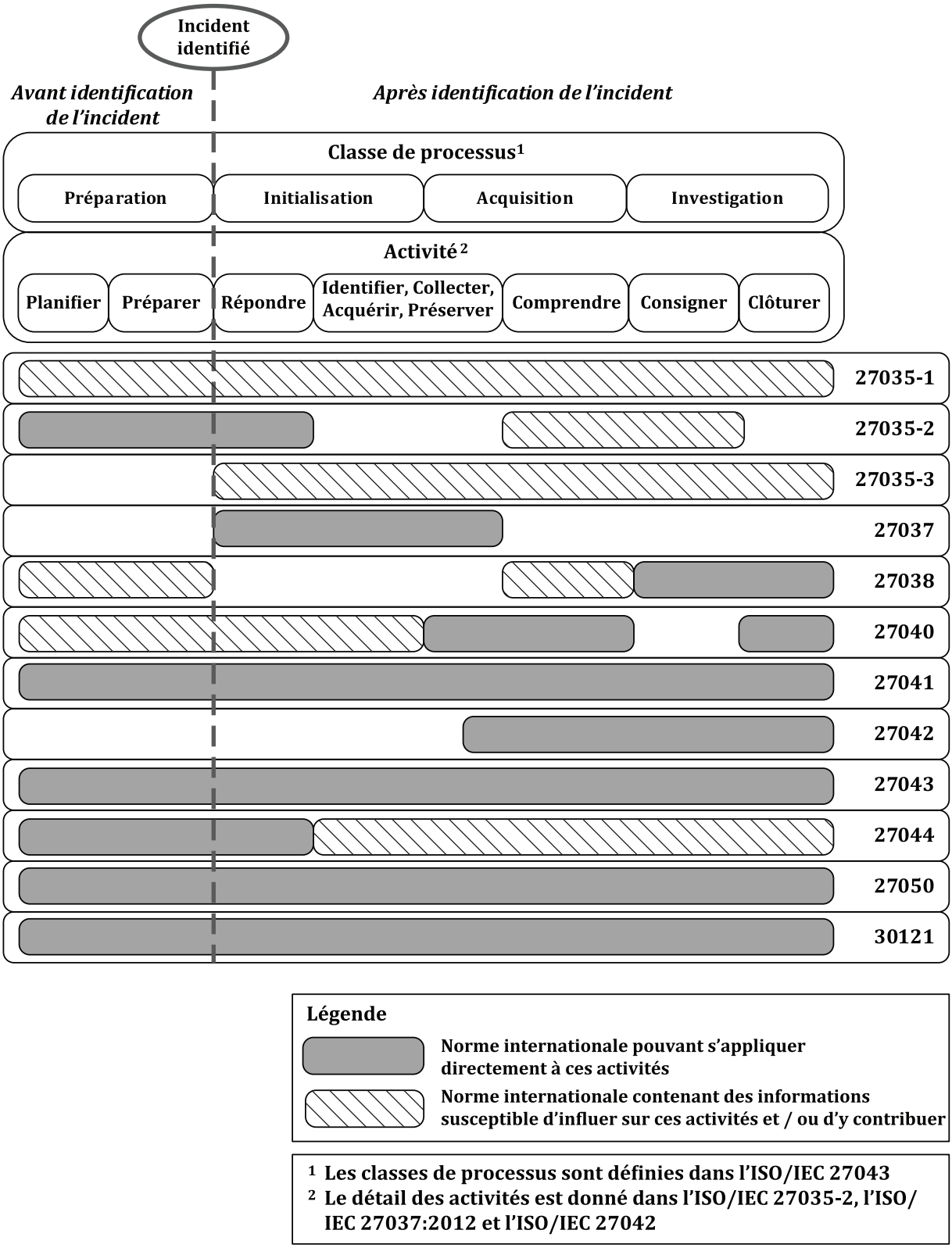

Figure 1 — Applicabilité des normes aux activités et classes des processus d'investigation

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'analyse et l'interprétation des preuves numériques

1 Domaine d'application

La présente Norme internationale fournit des préconisations concernant l'analyse et l'interprétation des preuves numériques d'une façon qui traite les problèmes de continuité, de validité, de reproductibilité et de répétabilité. Elle englobe les pratiques d'excellence sur la sélection, la conception et la mise en œuvre des processus analytiques et de consignation des informations suffisantes pour permettre la soumission de tels processus à un examen approfondi indépendant, si nécessaire. Elle fournit des préconisations concernant des mécanismes adéquats de démonstration de l'aptitude et de la compétence de l'équipe d'investigation.

L'analyse et l'interprétation des preuves numériques peuvent être un processus complexe. Dans certains cas, il peut exister plusieurs méthodes qui pourraient être appliquées et les membres de l'équipe d'investigation devront justifier leur sélection d'un processus donné et démontrer son équivalence par rapport à un autre processus utilisé par d'autres investigateurs. Dans d'autres cas, les investigateurs peuvent être obligés de concevoir de nouvelles méthodes d'examen des preuves numériques qui n'ont pas été envisagées auparavant et il convient qu'ils soient capables de démontrer que la méthode produite est «en adéquation avec l'application visée».

L'application d'une méthode spécifique peut influer sur l'interprétation des preuves numériques traitées avec cette méthode. Les preuves numériques disponibles peuvent influer sur la sélection des méthodes pour l'analyse ultérieure des preuves numériques qui ont déjà été acquises.

La présente Norme internationale fournit un cadre commun, pour les éléments d'analyse et d'interprétation de la gestion des incidents de sécurité des systèmes d'information qui peut être utilisé pour faciliter la mise en œuvre de nouvelles méthodes et fournir une norme commune minimale pour les preuves numériques produites à partir de telles activités.

2 Références normatives

Les documents ci-après, dans leur intégralité ou non, sont des références normatives indispensables à l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO/IEC 27000:2013, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire*

ISO/IEC 27037:2012, *Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques*

ISO/IEC 27041[4)], *Technologies de l'information — Techniques de sécurité — Préconisations concernant la garantie d'aptitude à l'emploi et d'adéquation des méthodes d'investigation sur incident*

4) Publication en attente