Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1541

(09/2012)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Echange d'informations sur la cybersécurité – Echange concernant les événements/les incidents/l'heuristique

Format d'échange de description d'objet incident

Recommandation UIT-T X.1541

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le pollupostage	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	**X.1540–X.1549**
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1541

Format d'échange de description d'objet incident

Résumé

La Recommandation UIT T X.1541 décrit le modèle d'information pour le format d'échange de description d'objet incident (IODEF, *incident object description exchange format*) et définit un modèle de données associé, spécifié en XML. Ce modèle est destiné à être utilisé pour le partage des informations sur les incidents en matière de sécurité informatique ou d'autres types d'incidents que s'échangent couramment les équipes d'intervention en cas d'incident relatif à la sécurité informatique et les fournisseurs de services. A cette fin, la présente Recommandation énumère les dispositions pertinentes de la norme IETF RFC 5070 et indique si elles ont un caractère normatif ou informatif.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T X.1541	2012-09-07	17

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Introduction

La Recommandation UIT-T X.1500 "Techniques d'échange d'informations sur la cybersécurité" fournit des lignes directrices relatives à l'échange d'informations sur la cybersécurité, y compris d'informations sur les incidents et les indicateurs, telles que celles fournies dans la présente Recommandation UIT-T. Le format d'échange de description d'objet incident (IODEF, *incident object description exchange format*) est un modèle de données permettant de représenter les informations sur la sécurité informatique couramment échangées. Il définit une représentation de modèle de données XML permettant d'acheminer des informations sur les incidents entre des entités qui, sur le plan opérationnel, sont chargées de mettre en place des parades préventives, de mener des activités de remise en état ou d'assurer un service de veille et d'alerte pour un public donné. Le modèle de données offre une méthode permettant de coder les informations sur les serveurs, les réseaux et les services exploités sur ces systèmes, sur la méthodologie d'exploitation et les données associées, sur les conséquences de l'incident et sur les démarches plus restrictives visant à documenter le déroulement des opérations.

L'objectif prioritaire du format IODEF est d'améliorer les capacités opérationnelles et les capacités d'évaluation d'une situation. L'adoption de ce format IODEF par la communauté renforce ses capacités de résoudre les incidents et d'acheminer des avertissements concernant les différentes menaces pour une situation donnée, en simplifiant la collaboration et le partage d'informations. Le format structuré IODEF permet:

- de renforcer l'automatisation du traitement des informations sur les incidents grâce à l'échange d'informations structurées sur les incidents, ce qui évite aux analystes de la sécurité d'avoir à examiner les textes de forme libre;
- de faciliter la mise en corrélation des données semblables (même très structurées) en provenance de sources différentes pour avoir une meilleure connaissance de la situation;
- de disposer d'un format commun à partir duquel il sera possible d'assurer l'interopérabilité des outils de traitement des incidents et d'analyse, en particulier lorsque les informations proviennent de plusieurs entités.

De nombreuses considérations politiques et juridiques liées aux procédures et à la confiance peuvent limiter ou empêcher l'échange d'informations. Le format IODEF est une spécification technique et n'a pas pour objet de traiter ces questions. La mise en œuvre opérationnelle du format IODEF et des formats et protocoles associés devrait néanmoins tenir compte de ce contexte plus général lors de la conclusion d'accords d'échange d'informations.

Recommandation UIT-T X.1541

Format d'échange de description d'objet incident

1 Domaine d'application

Le format d'échange de description d'objet incident (IODEF, *incident object description exchange format*) définit une représentation de modèle de données pour le partage des informations couramment échangées concernant les incidents en matière de sécurité informatique et d'autres types d'incidents (CSIRT, *computer security incident response team*). La présente Recommandation décrit le modèle d'information pour le format IODEF et fournit un modèle de données associé, spécifié pour le format XML.

Toute représentation de modèle de données ou tout cadre permettant l'échange d'informations sur des incidents relatifs à la sécurité informatique ou d'autres types d'incidents doit comprendre les fonctionnalités permettant de respecter toutes les législations, réglementations et politiques nationales ou régionales applicables.

Les responsables de la mise en œuvre et les utilisateurs de toutes les Recommandations UIT-T, y compris la présente Recommandation et les techniques sous-jacentes, doivent se conformer à toutes les législations, réglementations et politiques nationales ou régionales applicables.

2 Références

Les Recommandations UIT-T suivantes et les autres références contiennent des dispositions qui, en référence à ce texte, constituent les dispositions de cette Recommandation. A la date de publication de cette Recommandation, les éditions indiquées sont valides. Toutes les Recommandations et autres références sont susceptibles d'être révisées; les utilisateurs de la présente Recommandation sont donc encouragés à envisager la possibilité d'utiliser l'édition la plus récente des Recommandations et des autres références dont la liste figure ci-après. Une liste des Recommandations UIT-T actuellement en vigueur est publiée régulièrement. Toute référence à un document cité dans la présente Recommandation, considéré comme un document autonome, ne lui confère pas le statut de Recommandation.

[IETF RFC 5070] Norme RFC 5070 (2007) de l'IETF, *The Incident Object Description Exchange Format*. <http://datatracker.ietf.org/doc/RFC 5070/>

3 Définitions

3.1 Termes définis ailleurs

Aucun.

3.2 Termes définis dans la présente Recommandation

Aucun.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

IANA autorité chargée de l'assignation des numéros Internet (*Internet assigned numbers authority*)

IODEF format d'échange de description d'objet incident (*incident object description exchange format*)

5 Conventions

Les termes suivants sont considérés comme équivalents:

- À l'UIT, l'emploi du futur d'obligation ("shall" en anglais) est équivalent à celui d'autres moyens d'expression de l'obligation (comme "must" en anglais), la même chose valant pour leurs formes négatives.
- À l'UIT, l'emploi du futur d'obligation ("shall" en anglais) est équivalent à l'emploi à l'IETF du mot "MUST" en anglais.
- À l'UIT, l'emploi de la forme négative du futur d'obligation ("shall not" en anglais) est équivalent à l'emploi à l'IETF des mots "MUST NOT" en anglais.

NOTE – A l'IETF, les mots "shall" et "must" (en caractères minuscules) sont employés dans les textes informatifs.

6 Description d'objet incident et format d'échange

Le paragraphe 6 définit le format d'échange de description d'objet incident (IODEF, *incident object description exchange format*). Ce paragraphe fait directement référence à la norme [IETF RFC 5070]. Y sont mis en correspondance les numéros des paragraphes avec ceux des sections de manière que le paragraphe 6.x corresponde à la section x de la norme [IETF RFC 5070], leurs intitulés concordant aussi.

NOTE – Un erratum de la norme [b-IETF RFC 5070] est disponible dans [b-Errata ID3333].

6.1 Introduction

La section 1 de la norme [b-IETF RFC 5070] est informative.

6.1.1 Terminologie

La section 1.1 de la norme [b-IETF RFC 5070] est informative.

6.1.2 Notations

La section 1.2 de la norme [b-IETF RFC 5070] est informative.

6.1.3 Concernant le modèle de données IODEF

La section 1.3 de la norme [b-IETF RFC 5070] est informative.

6.1.4 Concernant la mise en œuvre IODEF

La section 1.4 de la norme [b-IETF RFC 5070] est informative.

6.2 Types de données IODEF

La section 2 de la norme [b-IETF RFC 5070] est informative.

6.2.1 Entiers

La section 2.1 de la norme [IETF RFC 5070] est normative.

6.2.2 Nombres réels

La section 2.2 de la norme [IETF RFC 5070] est normative.

6.2.3 Caractères et chaînes

La section 2.3 de la norme [IETF RFC 5070] est normative.

6.2.4 Chaînes multilingues

La section 2.4 de la norme [IETF RFC 5070] est normative.

6.2.5 Octets

La section 2.5 de la norme [IETF RFC 5070] est normative.

6.2.6 Octets hexadécimaux

La section 2.6 de la norme [IETF RFC 5070] est normative.

6.2.7 Types énumérés

La section 2.7 de la norme [IETF RFC 5070] est normative.

6.2.8 Chaînes d'horodatage

La section 2.8 de la norme [IETF RFC 5070] est normative.

6.2.9 Chaîne de fuseau horaire

La section 2.9 de la norme [IETF RFC 5070] est normative.

6.2.10 Listes des ports

La section 2.10 de la norme [IETF RFC 5070] est normative.

6.2.11 Adresse postale

La section 2.11 de la norme [IETF RFC 5070] est normative.

6.2.12 Personne ou organisme

La section 2.12 de la norme [IETF RFC 5070] est normative.

6.2.13 Numéros de téléphone et de télécopie

La section 2.13 de la norme [IETF RFC 5070] est normative.

6.2.14 Chaîne d'adresse électronique

La section 2.14 de la norme [IETF RFC 5070] est normative.

6.2.15 Chaînes d'adresses URL

La section 2.15 de la norme [IETF RFC 5070] est normative.

6.3 Modèle de données IODEF

La section 3 de la norme [b-IETF RFC 5070] est informative.

6.3.1 Classe IODEF-document

La section 3.1 de la norme [IETF RFC 5070] est normative.

6.3.2 Classe Incident

La section 3.2 de la norme [IETF RFC 5070] est normative.

6.3.3 Classe IncidentID

La section 3.3 de la norme [IETF RFC 5070] est normative.

6.3.4 Classe AlternativeID

La section 3.4 de la norme [IETF RFC 5070] est normative.

6.3.5 Classe RelatedActivity

La section 3.5 de la norme [IETF RFC 5070] est normative.

6.3.6 Classe AdditionalData

La section 3.6 de la norme [IETF RFC 5070] est normative.

6.3.7 Classe Contact

La section 3.7 de la norme [IETF RFC 5070] est normative.

6.3.7.1 Classe RegistryHandle

La section 3.7.1 de la norme [IETF RFC 5070] est normative.

6.3.7.2 Classe PostalAddress

La section 3.7.2 de la norme [IETF RFC 5070] est normative.

6.3.7.3 Classe Email

La section 3.7.3 de la norme [IETF RFC 5070] est normative.

6.3.7.4 Classes Telephone et Fax

La section 3.7.4 de la norme [IETF RFC 5070] est normative.

6.3.8 Classes Time

La section 3.8 de la norme [IETF RFC 5070] est normative.

6.3.8.1 StartTime

La section 3.8.1 de la norme [IETF RFC 5070] est normative.

6.3.8.2 EndTime

La section 3.8.2 de la norme [IETF RFC 5070] est normative.

6.3.8.3 DetectTime

La section 3.8.3 de la norme [IETF RFC 5070] est normative.

6.3.8.4 ReportTime

La section 3.8.4 de la norme [IETF RFC 5070] est normative.

6.3.8.5 DateTime

La section 3.8.5 de la norme [IETF RFC 5070] est normative.

6.3.9 Classe Method

La section 3.9 de la norme [IETF RFC 5070] est normative.

6.3.9.1 Classe Reference

La section 3.9.1 de la norme [IETF RFC 5070] est normative.

6.3.10 Classe Assessment

La section 3.10 de la norme [IETF RFC 5070] est normative.

6.3.10.1 Classe Impact

La section 3.10.1 de la norme [IETF RFC 5070] est normative.

6.3.10.2 Classe TimeImpact

La section 3.10.2 de la norme [IETF RFC 5070] est normative.

6.3.10.3 Classe MonetaryImpact

La section 3.10.3 de la norme [IETF RFC 5070] est normative.

6.3.10.4 Classe Confidence

La section 3.10.4 de la norme [IETF RFC 5070] est normative.

6.3.11 Classe History

La section 3.11 de la norme [IETF RFC 5070] est normative.

6.3.11.1 Classe HistoryItem

La section 3.11.1 de la norme [IETF RFC 5070] est normative.

6.3.12 Classe EventData

La section 3.12 de la norme [IETF RFC 5070] est normative.

6.3.12.1 Classes Relating the Incident et EventData

La section 3.12.1 de la norme [IETF RFC 5070] est normative.

6.3.12.2 Cardinality of EventData

La section 3.12.2 de la norme [IETF RFC 5070] est normative.

6.3.13 Classe Expectation

La section 3.13 de la norme [IETF RFC 5070] est normative.

6.3.14 Classe Flow

La section 3.14 de la norme [IETF RFC 5070] est normative.

6.3.15 Classe System

La section 3.15 de la norme [IETF RFC 5070] est normative.

6.3.16 Classe Node

La section 3.16 de la norme [IETF RFC 5070] est normative.

6.3.16.1 Classe Counter

La section 3.16.1 de la norme [IETF RFC 5070] est normative.

6.3.16.2 Classe Address

La section 3.16.2 de la norme [IETF RFC 5070] est normative.

6.3.16.3 Classe NodeRole

La section 3.16.3 de la norme [IETF RFC 5070] est normative.

6.3.17 Classe Service

La section 3.17 de la norme [IETF RFC 5070] est normative.

6.3.17.1 Classe Application

La section 3.17.1 de la norme [IETF RFC 5070] est normative.

6.3.18 Classe OperatingSystem

La section 3.18 de la norme [IETF RFC 5070] est normative.

6.3.19 Classe Record

La section 3.19 de la norme [IETF RFC 5070] est normative.

6.3.19.1 Classe RecordData

La section 3.19.1 de la norme [IETF RFC 5070] est normative.

6.3.19.2 Classe RecordPattern

La section 3.19.2 de la norme [IETF RFC 5070] est normative.

6.3.19.3 Classe RecordItem

La section 3.19.3 de la norme [IETF RFC 5070] est normative.

6.4 Considérations relatives au traitement

La section 4 de la norme [b-IETF RFC 5070] est informative.

6.4.1 Codage

La section 4.1 de la norme [IETF RFC 5070] est normative.

6.4.2 Espace de nom IODEF

La section 4.2 de la norme [IETF RFC 5070] est normative.

6.4.3 Validation

La section 4.3 de la norme [IETF RFC 5070] est normative.

6.5 Extension du format IODEF

La section 5 de la norme [b-IETF RFC 5070] est informative.

La Recommandation UIT-T X.1500 "Techniques d'échange d'informations sur la cybersécurité" fournit des lignes directrices relatives à l'échange d'informations sur les incidents et les indicateurs, telles que celles fournies dans la présente Recommandation. La présente Recommandation donne le format de base pour l'échange d'informations sur les incidents, mais ne couvre pas tous les types d'utilisation conformément à la Recommandation UIT-T X.1500. Il faudra peut-être définir des extensions pour couvrir les types d'utilisation requis.

6.5.1 Extension des valeurs énumérées des attributs

La section 5.1 de la norme [IETF RFC 5070] est normative.

6.5.2 Extension des classes

La section 5.2 de la norme [IETF RFC 5070] est normative.

6.6 Questions liées à l'internationalisation

La section 6 de la norme [IETF RFC 5070] est normative.

6.7 Exemples

La section 7 de la norme [b-IETF RFC 5070] est informative.

6.7.1 Vers

La section 7.1 de la norme [b-IETF RFC 5070] est informative.

6.7.2 Reconnaissance

La section 7.2 de la norme [b-IETF RFC 5070] est informative.

6.7.3 Signalement des réseaux de robots

La section 7.3 de la norme [b-IETF RFC 5070] est informative.

6.7.4 Liste de surveillance

La section 7.4 de la norme [b-IETF RFC 5070] est informative.

6.8 Le schéma IODEF

La section 8 de la norme [IETF RFC 5070] est normative.

6.9 Considérations relatives à la sécurité

La section 9 de la norme [IETF RFC 5070] est normative.

Dans les mises en œuvre conformes aux normes de l'UIT-T, le format de messagerie et le protocole sous-jacents utilisés pour l'échange d'instances du format IODEF doivent offrir les garanties nécessaires de confidentialité, d'intégrité et d'authenticité.

NOTE – À l'IETF, le mot "must" (en caractères minuscules) est employé dans les textes informatifs.

6.10 Considérations de l'autorité IANA

La section 10 de la norme [IETF RFC 5070] est normative.

6.11 Remerciements

La section 11 de la norme [b-IETF RFC 5070] est informative.

6.12 Références

6.12.1 Normative

La section 12.1 de la norme [b-IETF RFC 5070] est informative.

Selon la présente Recommandation UIT-T, la section 12 de la norme [IETF RFC 5070] est informative, car l'UIT-T n'a pas arrêté de position sur ces références en ce qui concerne la présente Recommandation. Toutefois, il est admis que l'IETF a identifié un ensemble de références normatives pour la norme [IETF RFC 5070].

6.12.2 Informative

La section 12.2 de la norme [b-IETF RFC 5070] est informative.

Bibliographie

[b-UIT-T X.1500] Recommandation UIT-T X.1500 (2011), *Techniques d'échange d'informations sur la cybersécurité*.

[b-Errata ID3333] IETF RFC Errata ID: 3333 de l'IETF, IETF RFC5070, *"The Incident Object Description Exchange Format", décembre 2007; statut: en cours de mise à jour; type: rédactionnelle; date indiquée: 02/09/2012*. <http://www.rfc-editor.org/errata_search.php?eid=3333>

[b-IETF RFC 5070] Norme RFC 5070 de l'IETF (2007), *Incident Object Description Exchange Format (IODEF)*. <https://datatracker.ietf.org/doc/RFC 5070/>

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2013