Quality Excellence for Suppliers of

Telecommunications Forum

(QuEST Forum)

TL 9000
Quality Management System

Security Measurements Guidance Document

Release 1.0

TL 9000 Security Measurements Guidance Document

Quality Excellence for Suppliers of

Telecommunications Forum

(QuEST Forum)

TL9000
品質マネジメントシステム

セキュリティ測定法ガイダンス文書

Release 1.0

[訳注：本書原文は http://tl9000.org/resources/documents/Security_Measurements_Guidance_Document_v1.0.doc 参照]

Introduction

QuEST Forum's vision is to be the global force for improving quality of products and services delivered to customers of communication technologies. It is a unique collaboration of service providers, suppliers and liaison organizations who come together to develop innovative solutions to practical business problems that make a difference to end users. As the communications industry continues to evolve and introduce new technologies, QuEST forum continues to use its expertise of the last two decades, through industry–wide collaboration to address these new challenges.

The Executive Board chartered the Next Generation Measurements Security Sub Team to identify existing industry security measurements. Based on a study of various Standards Development Organizations (SDOs), the published measurements from Center for Internet Security (CIS)*1 http://www.cisecurity.org and National Institute for Standards and Technology (NIST) http://www.nist.gov/index.html were found to be most relevant to our efforts. The team also examined in detail the work of the Cloud Security Alliance (CSA) SDO on security measurements. However, their work is still in-progress.

The measurements referenced from NIST and CIS are operational measurements applicable to an operations environment (not a development environment or supply chain) for the purpose of monitoring the effectiveness of security management within that operation. Some of these measurements may need modification before application to a telecommunications operations environment. As such, the measurements described here provide a basis for future work which can include trialing of use of the measurement, refinement of the definition, and wider review against other similar measurements that may be identified in the industry.

The QuEST Forum has paraphrased the CIS and NIST measurements to conform to the TL 9000 format. To review the original measurements, the reader is directed to the links provided above and in the footnote.

In publishing this document, the Next Generation Measurements Security Sub Team expects it will enable the TL 9000 registered organizations' continual improvement of the security of their products and services.

These measurements are for guidance only, and not intended to be mandatory for TL 9000 certification.

Most Relevant Measurements

The identified existing security measurements were not developed by SDOs specifically for the telecommunications industry in the spirit of TL 9000. For example, the NIST security measures assess the security assurance level of an organization regarding its information system management, operations and technology rather than focusing on a supplier's product security benchmarking. Some third party assessment/scanning tools are also needed. Most of the source data comes from incident databases, IDS logs and alerts which are from security suppliers who are usually not telecommunication manufacturers. The identified measurements are useful since they focus on measuring the security recovery and adaptation capabilities of the products and the network. Examples of such measurements are "Percentage of Systems without Known Severe Vulnerabilities" or "Mean-Time to Mitigate Vulnerabilities." However, due to the complex telecommunications scenario both in the technical and contractual context, compared to the IT world, it is not very clear whether such measures will be eagerly adopted at this stage by the TL 9000 registered companies.

Thus, the team has made an effort to identify measurements which will have high relevance for the TL 9000 user. It is hoped these most relevant measurements will significantly improve a user's security posture by their use in the tracking and benchmarking of product security. The most relevant measurements are identified in the right-most column of the two "Table of Contents" tables below. The tables are sorted by Measurement Number and by Category.

*1 CIS Consensus Security Metrics developed by the Security Benchmarks Division
http://benchmarks.cisecurity.org/en-us/?route=downloads.show.single.metrics.110

はじめに

クエストフォーラムのビジョンは，情報通信技術利用のお客様へ提供する製品及びサービスの品質向上のためのグローバルな推進力となることである。エンドユーザに影響を与える実務上のビジネスの問題に対して，サービスプロバイダ，供給者，さらには連携関係にある機関が協調するユニークな存在となっている。通信産業が発展し新技術を導入していく中，クエストフォーラムは，業界全体でこれらの新しいチャレンジに取り組み，過去 20 年間に亘り，その専門知識を活用し続けている。

クエストフォーラムの理事会は，業界の既存のセキュリティ測定法を確認するために，次世代セキュリティ測定法サブチームを設立した。
様々な規格開発機関（Standards Development Organizations (SDOs)）の調査の結果，米国インターネットセキュリティセンター（Center for Internet Security (CIS) *1 http://www.cisecurity.org）及び米国国立標準技術研究所（National Institute for Standards and Technology (NIST) http://www.nist.gov/index.html）から刊行されている測定法が，我々の努力に最も関連が深いということが分かった。チームはまた，クラウドセキュリティアライアンス（Cloud Security Alliance (CSA)）のセキュリティ測定法の研究についても詳細に調査した。ただし，それらの研究はまだ進行中である。

NIST と CIS から参照された測定法は，運用環境（開発環境でもサプライチェーンでもなく）に適用し，運用環境下でセキュリティマネジメントが効果的に働いているかどうかを監視する目的で利用できるものである。これらの測定法のいくつかは，通信技術の運用環境に適用する前に，修正が必要かもしれない。したがって，ここで説明される測定法は，測定法利用試験や，その定義の修正，業界で定められるかもしれない他の類似の測定法に対するより広範囲のレビューのような，今後の研究への基盤を提供している。

クエストフォーラムは CIS と NIST の測定法を TL 9000 の形式に合わせて，分かりやすく言い換えた。
なお，オリジナルの測定法については，上記及び脚注のリンクから参照可能。

この文書の出版により，次世代セキュリティ測定法サブチームは，TL9000 に登録している組織の製品及びサービスのセキュリティが継続的に改善されるようになることを期待している。

これらの測定法は，ガイダンスとなることのみを目的としており，TL 9000 認証に必須となることを意図していない。

最も関連性の深い測定法

既存のセキュリティ測定法は，TL 9000 の理念である電気通信業界をターゲットとして，規格開発機関（SDOs）により開発されたものではない。例えば NIST のセキュリティ測定法は，供給者の製品のセキュリティのベンチマーク化に焦点を当てているというよりは，情報システムの管理，運用，技術に観点を置き，組織のセキュリティ保証のレベルを評価している。いくつかの第三者機関の評価/スキャンツールも必要である。元となるデータのほとんどは，通常は通信機器製造業ではないセキュリティ製品供給者から提供されるインシデント・データベース，IDS のログや警報である。
これらの測定法は，製品やネットワークのセキュリティ復旧や対応能力の測定に焦点を当てている点から，役に立つ。その測定法の例としては，「既知の深刻な脆弱性が無いシステムの比率」や「平均脆弱性軽減時間」がある。しかし，IT の世界と比べ，技術面及び契約面の両面において複雑な電気通信の状況ゆえ，これらの測定法が，TL 9000 の登録企業によって現段階で積極的に採用されるかどうかは，定かではない。

そのためチームは，TL 9000 ユーザのために，関連性の深い測定法を特定することに努力してきた。最も関連性の深い測定法が，製品セキュリティのトラッキングやベンチマークに用いられることにより，TL 9000 ユーザのセキュリティ体制を著しく改善することが望まれている。最も関連性の深い測定法は，下記の 2 つの目次の表の最右列で確認できる。その表は測定法番号と分類によって整理 されている。

*1 セキュリティ・ベンチマーク部により開発された「合意のセキュリティ測定法（CIS:Consensus Security Metrics）」
http://benchmarks.cisecurity.org/en-us/?route=downloads.show.single.metrics.110

Table of Contents (Sorted by Measurement Number)

TL 9000 Security Measurements Guidance Document

目次 (測定法番号による整理)

Release 1.0 Page 3 July 2012

Table of Contents (Sorted by Category)

Measurement Number	Measurement ID	Source	Measurement Name	Category	Most Relevant
1.12	RAC	CIS	Risk Assessment Coverage	Applications	
1.13	STC	CIS	Security Testing Coverage	Applications	Yes
2.2	RACM	NIST	Remote Access Control Measure	Attacks	
1.8	PCC	CIS	Percentage of Configuration Compliance	Configuration	
1.9	MTTC	CIS	Mean Time to Complete Changes	Configuration	
1.10	PCSR	CIS	Percent of Changes with Security Review	Configuration	
1.11	PCSE	CIS	Percent of Changes with Security Exceptions	Configuration	
2.6	CCM	NIST	Configuration Changes Measure	Configuration	Yes
2.16	SCPM	NIST	System and Communication Protection Measure	Crypto	Yes
2.3	STM	NIST	Security Training Measure	Governance	
2.4	ARRM	NIST	Audit Record Review Measure	Governance	Yes
2.5	CACM	NIST	Certification and Accreditation (C&A) Completion Measure	Governance	
2.7	CPTM	NIST	Contingency Plan Testing Measure	Governance	
2.12	PM	NIST	Planning Measure	Governance	
2.13	PSM	NIST	Personnel Security Measure	Governance	
2.15	SACM	NIST	Service Acquisition Contract Measure	Governance	
2.8	UAM	NIST	User Accounts Measure	Governance	
1.1	MTTID	CIS	Mean Time to Incident Discovery	Incidents	Yes
1.2	MTBSI	CIS	Mean Time Between Security Incidents	Incidents	Yes
1.3	MTIR	CIS	Mean Time to Incident Recovery	Incidents	Yes
2.9	IRM	NIST	Incident Response Measure	Incidents	Yes
2.11	PSIM	NIST	Physical Security Incidents Measure	Incidents	
3.1	SRO	QF	Security Related Outages	Incidents	Yes
2.10	MSM	NIST	Media Sanitization Measure	Maintenance	
1.6	PPC	CIS	Patch Policy Compliance	Patching	
1.7	MTTP	CIS	Mean Time to Patch	Patching	Yes
1.4	PSWKSV	CIS	Percent of Systems Without Known Severe Vulnerabilities	Vulnerability	Yes
1.5	MTTMV	CIS	Mean-Time to Mitigate Vulnerabilities	Vulnerability	Yes
2.1	VM	NIST	Vulnerability Measure	Vulnerability	Yes
2.14	RAVM	NIST	Risk Assessment Vulnerability Measure	Vulnerability	Yes
2.17	FRM	NIST	Flaw Remediation Measure	Vulnerability	Yes

TL 9000 Security Measurements Guidance Document

目次 (分類による整理)

測定法番号	測定法識別子	ソース	測定法名称	分類	関連性
1.12	RAC	CIS	リスクアセスメント適用率	アプリケーション	
1.13	STC	CIS	セキュリティ試験適用率	アプリケーション	有り
2.2	RACM	NIST	リモートアクセス制御測定	攻撃	
1.8	PCC	CIS	構成適合性比率	構成	
1.9	MTTC	CIS	平均変更完了時間	構成	
1.10	PCSR	CIS	セキュリティレビュー変更比率	構成	
1.11	PCSE	CIS	セキュリティ除外変更比率	構成	
2.6	CCM	NIST	構成変更測定	構成	有り
2.16	SCPM	NIST	システム及び通信保護測定	クリプト	有り
2.3	STM	NIST	セキュリティ教育・訓練測定	ガバナンス	
2.4	ARRM	NIST	監査記録レビュー測定	ガバナンス	有り
2.5	CACM	NIST	認証及び認定（C&A）完了測定	ガバナンス	
2.7	CPTM	NIST	緊急時対応計画試験測定	ガバナンス	
2.12	PM	NIST	計画作成測定	ガバナンス	
2.13	PSM	NIST	要員セキュリティ測定	ガバナンス	
2.15	SACM	NIST	サービス調達契約測定	ガバナンス	
2.8	UAM	NIST	ユーザアカウント測定	ガバナンス	
1.1	MTTID	CIS	平均インシデント検出時間	インシデント	有り
1.2	MTBSI	CIS	平均セキュリティインシデント間隔時間	インシデント	有り
1.3	MTIR	CIS	平均インシデント復旧時間	インシデント	有り
2.9	IRM	NIST	インシデント対応測定	インシデント	有り
2.11	PSIM	NIST	物理的セキュリティインシデント測定	インシデント	
3.1	SRO	QF	セキュリティ関連停止	インシデント	有り
2.10	MSM	NIST	媒体上の記録抹消測定	保守	
1.6	PPC	CIS	パッチ方針適合性	パッチ	
1.7	MTTP	CIS	平均パッチ時間	パッチ	有り
1.4	PSWKSV	CIS	既知の深刻な脆弱性がないシステムの比率	脆弱性	有り
1.5	MTTMV	CIS	平均脆弱性軽減時間	脆弱性	有り
2.1	VM	NIST	脆弱性測定	脆弱性	有り
2.14	RAVM	NIST	脆弱性リスクアセスメント測定	脆弱性	有り
2.17	FRM	NIST	欠陥修正測定	脆弱性	有り

Release 1.0 Page4 July 2012

1.1 Mean Time to Incident Discovery

1.1.1 General Description and Title

Mean-Time-To-Incident-Discovery (MTTID) measures the effectiveness of the organization in detecting security incidents. Generally, the faster an organization can detects an incident, the less damage it is likely to incur. MTTID is the average amount of time, in hours, that elapsed between the Date of Occurrence and the Date of Discovery for a given set of incidents. The calculation can be averaged across a time period, type of incident, business unit, or severity.

1.1.2 Purpose

Mean-Time-To-Incident-Discovery (MTTID) characterizes the efficiency of detecting incidents, by measuring the average elapsed time between the initial occurrence of an incident and its subsequent discovery. The MTTID metric also serves as a leading indicator of resilience in organization defenses because it measures detection of attacks from known vectors and unknown ones.

1.1.3 Applicable Categories

Core Network Products and End Customer Services. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

1.1.4 Detailed Description

a) Terminology

Security Incident – A security incident results in the actual outcomes of a business process deviating from the expected outcomes for confidentiality, integrity & availability due to deficiencies or failures of people, process or technology.

b) Counting Rules:

Only incidents that meet the above definition of Security Incident should be included.

These would be manual inputs as defined in CIS document Security Incident Metrics: Data Attributes

c) Counting Rule Exclusions:

Incidents that should not be considered “security incidents” include disruption of service due to equipment failures.

d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
MTTID	Mean Time to Incident Discovery	Sigma (Date_of_Discovery - Date_of_Occurrence) / Count(Incidents)	Hours per Incident

1.1.5 Sources of Data

Since humans determine when an incident occurs, when the incident is contained, and when the incident is resolved, the primary data sources for this metric are manual inputs as defined in Security Incident Metrics: Data Attributes. However, these incidents may be reported by operational security systems, such as anti-malware software, security incident and event management (SIEM) systems, and host logs.

1.1.6 Reporting Frequency

Weekly is recommended but can be reported Monthly, Quarterly or Annually

1.1.7 Source of Measurement

CIS

1.1 平均インシデント検出時間

1.1.1 一般

平均インシデント検出時間（MTTID）は，組織のセキュリティインシデント検出の有効性を測定する。一般に，組織がより速くインシデントを検出できれば，被る損害を小さくすることができる。MTTID は，あるインシデント群に関して，個々のインシデントの発生日と検出日の間で経過した時間を平均した時間（hour）を単位とする値である。期間，インシデントの種類，事業単位，又は重大性の観点から平均値を計算できる。

1.1.2 目的

平均インシデント検出時間（MTTID）は，インシデントの最初の発生からそれに続く検出までの間の平均経過時間を測定することによって，インシデントの検出能力を特徴付ける。MTTID の測定はまた，既知及び未知の方向（ベクトル）からの攻撃の検出を測定するので，組織防衛における回復力の先行指標となる。

1.1.3 適用する製品分類

コアネットワーク製品及びエンドユーザサービス。製品分類表の最新版は http://tl9000.org/resources/resources.html を参照。

1.1.4 詳細説明

a) 用語

セキュリティインシデント ー セキュリティインシデントは，人，プロセス，技術の欠陥又は不具合により，機密性，完全性及び可用性における，期待される結果に対し，実際のビジネスプロセスの結果に相違をもたらす。

b) 計数ルール

セキュリティインシデントの上記の定義に合うインシデントだけを含むこと。
これらは CIS 文書のセキュリティインシデント測定法「データ属性」に定義されているように手動入力である。

c) 計数ルールの除外

"セキュリティインシデント"と考えるべきではないインシデントには，機器障害によるサービスの中断を含む。

d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
MTTID	平均インシデント検出時間	Σ(検出日ー発生日) / インシデント数	インシデントごとの時間

1.1.5 データ発生源

いつインシデントが発生したか，いつインシデントが封じ込められたか，いつインシデントが解消したかは人が判断するので，この測定法の主要なデータ発生源は，セキュリティインシデント測定法「データ属性」に定義されているように手動入力である。しかし，これらのインシデントは，アンチマルウェア ソフトウェア，セキュリティインシデント及びイベント管理（SIEM）システム，及びホストログなどの運用セキュリティシステムによって報告されてもよい。

1.1.6 報告頻度

週次を推奨するが，月次，四半期又は年次報告でも良い。

1.1.7 測定法出典

CIS

1.2 Mean Time Between Security Incidents

1.2.1 General Description and Title

Mean Time Between Security Incidents (MTBSI) calculates the average time, in days, between security incidents.

1.2.2 Purpose

Mean Time Between Security Incidents (MTBSI) identifies the relative levels of security incident activity.

1.2.3 Applicable Categories

Core Network Products and End Customer Services. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

1.2.4 Detailed Description

a) Terminology

Security Incident – A security incident results in the actual outcomes of a business process deviating from the expected outcomes for confidentiality, integrity & availability due to deficiencies or failures of people, process or technology.

b) Counting Rules

Only incidents that meet the above definition of Security Incident should be included.

These would be manual inputs as defined in CIS document Security Incident Metrics: Data Attributes

c) Counting Rule Exclusions

Incidents that should not be considered “security incidents” include disruption of service due to equipment failures.

d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
MTBSI	Mean Time Between Security Incidents	Sigma ((Date_of_Occurence[Incident_n] □ Date_of_Occurence[Incident _n_minus_□1□])/ Count(Incidents)	Hours per incident interval

1.2.5 Sources of Data

Since humans determine when an incident occurs, when the incident is contained, and when the incident is resolved, the primary data sources for this metric are manual inputs as defined in Security Incident Metrics: Data Attributes. However, these incidents may be reported by operational security systems, such as anti-malware software, security incident and event management (SIEM) systems, and host logs.

1.2.6 Reporting Frequency

Weekly is recommended but can be reported Monthly, Quarterly or Annually

1.2.7 Source of Measurement

CIS

1.2 平均セキュリティインシデント間隔時間

1.2.1 一般

平均セキュリティインシデント間隔時間（MTBSI)はセキュリティインシデント間の平均時間で，日を単位として計算する。

1.2.2 目的

平均セキュリティインシデント間隔時間（MTBSI)は，セキュリティインシデント活動の相対的なレベルを示す。

1.2.3 適用する製品分類

コアネットワーク製品及びエンドユーザサービス。製品分類表の最新版は http://tl9000.org/resources/resources.html を参照。

1.2.4 詳細説明

a) 用語

セキュリティインシデント － セキュリティインシデントは，人，プロセス，技術の欠陥又は不具合により，機密性，完全性及び可用性における，期待される結果に対し，実際のビジネスプロセスの結果に相違をもたらす。

b) 計数ルール

セキュリティインシデントの上記の定義に合うインシデントだけを含むこと。

CIS 文書のセキュリティインシデント測定法「データ属性」に定義されているように手動入力である。

c) 計数ルールの除外

"セキュリティインシデント"と考えるべきではないインシデントには，機器障害によるサービスの中断を含む。

d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
MTBSI	平均セキュリティインシデント間隔時間	Σ(発生日[インシデント_n] － 発生日[インシデント_n-1]) / インシデント数	インシデント間隔時間(単位は日)

訳注：英文の注は Hours per incident interval とあるが，Days の誤り

1.2.5 データ発生源

いつインシデントが発生したか，いつインシデントが封じ込められたか，いつインシデントが解消したかは人が判断するので，この測定法の主要なデータ発生源は，セキュリティインシデント測定法「データ属性」に定義されているように手動入力である。しかし，これらのインシデントは，アンチマルウェア ソフトウェア，セキュリティインシデント及びイベント管理（SIEM）システム及びホストログなどの運用セキュリティシステムによって報告されてもよい。

1.2.6 報告頻度

週次を推奨するが，月次，四半期又は年次報告でも良い。

1.2.7 測定法出典

CIS

1.3 Mean Time to Incident Recovery

1.3.1 General Description and Title

Mean Time to Incident Recovery (MTIR) measures the effectiveness of the organization to recovery from security incidents. The sooner the organization can recover from a security incident, the less impact the incident will have on the overall organization. This calculation can be averaged across a time period, type of incident, business unit, or severity.

1.3.2 Purpose

Mean Time to Incident Recovery (MTIR) characterizes the ability of the organization to return to a normal state of operations. This is measured by the average elapse time between when the incident occurred to when the organization recovered from the incident.

1.3.3 Applicable Categories

Core Network Products and End Customer Services. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

1.3.4 Detailed Description

a) Terminology

Security Incident – A security incident results in the actual outcomes of a business process deviating from the expected outcomes for confidentiality, integrity & availability due to deficiencies or failures of people, process or technology.

b) Counting Rules

Only incidents that meet the above definition of Security Incident should be included.

These would be manual inputs as defined in CIS document Security Incident Metrics: Data Attributes

c) Counting Rule Exclusions

Incidents that should not be considered “security incidents” include disruption of service due to equipment failures.

d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
MTIR	Mean Time to Incident Recovery	Sigma (Date_of_Recovery - Date_of_Occurrence)/ Count(Incidents)	Hours per incident

1.3.5 Sources of Data

Since humans determine when an incident occurs, when the incident is contained, and when the incident is resolved, the primary data sources for this metric are manual inputs as defined in Security Incident Metrics: Data Attributes. However, these incidents may be reported by operational security systems, such as anti-malware software, security incident and event management (SIEM) systems, and host logs.

1.3.6 Reporting Frequency

Weekly is recommended but can be reported Monthly, Quarterly or Annually

1.3.7 Source of Measurement

CIS

1.3 平均インシデント復旧時間

1.3.1 一般

平均インシデント復旧時間（MTIR）は，セキュリティインシデントからの回復に対する組織の有効性を測定する。組織が迅速にセキュリティインシデントから立ち直ることができるほど，組織全体へのインシデントの影響は少なくなる。期間，インシデントの種類，事業単位，又は重大性の観点から平均値を計算できる。

1.3.2 目的

平均インシデント復旧時間（MTIR）は，業務を正常な運用状態に戻す為の組織の能力を特徴付ける。ここでは，インシデントの発生時から，組織がインシデントから回復した時までの平均経過時間を測定する。

1.3.3 適用する製品分類

コアネットワーク製品及びエンドユーザサービス。製品分類表の最新版は http://tl9000.org/resources/resources.html を参照。

1.3.4 詳細説明

a) 用語
セキュリティインシデント ー セキュリティインシデントは，人，プロセス，技術の欠陥又は不具合により，機密性，完全性及び可用性における，期待される結果に対し，実際のビジネスプロセスの結果に相違をもたらす。

b) 計数ルール
セキュリティインシデントの上記の定義に合うインシデントだけを含むこと。
CIS 文書のセキュリティインシデント測定法「データ属性」に定義されているように手動入力である。

c) 計数ルールの除外
"セキュリティインシデント"と考えるべきではないインシデントには，機器障害によるサービスの中断を含む。

d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
MTIR	平均インシデント復旧時間	Σ(回復日ー発生日) / インシデント数	インシデント毎ごとの時間

1.3.5 データ発生源

いつインシデントが発生したか，いつインシデントが封じ込められたか，いつインシデントが解消したかは人が判断するので，この測定法の主要なデータ発生源は，セキュリティインシデント測定法「データ属性」に定義されているように手動入力である。しかし，これらのインシデントは，アンチマルウェア ソフトウェア，セキュリティインシデント及びイベント管理（SIEM）システム，及びホストログなどの運用セキュリティシステムによって報告されてもよい。

1.3.6 報告頻度

週次を推奨するが，月次，四半期又は年次報告でも良い

1.3.7 測定法出典

CIS

1.4 Percent of Systems without Known Severe Vulnerabilities

1.4.1 General Description and Title

Percent of Systems without Known Severe Vulnerabilities (PSWKSV) measures the percentage of systems that when checked were not found to have any known high severity vulnerabilities during a vulnerability scan.

Since vulnerability management involves both the identification of new severe vulnerabilities and the remediation of known severe vulnerabilities, the percentage of systems without known severe vulnerabilities will vary over time. Organizations can use this metric to gauge their relative level of exposure to exploits and serves as a potential indicator of expected levels of security incidents (and therefore impacts on the organization).

This severity threshold is important, as there are numerous informational, local, and exposure vulnerabilities that can be detected that are not necessarily material to the organization's risk profile. Managers generally will want to reduce the level of noise to focus on the greater risks first. This metric can also be calculated for subsets of systems, such as by asset criticality of business unit.

1.4.2 Purpose

Percent of Systems without Known Severe Vulnerabilities (PSWKSV) measures the organization's relative exposure to known severe vulnerabilities. The metric evaluates the percentage of systems scanned that do not have any known high severity vulnerabilities.

1.4.3 Applicable Categories

Core Network Products and End Customer Services. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

1.4.4 Detailed Description

a) Terminology

Vulnerability -- Vulnerability is defined as a weakness that could be exploited by an attacker to gain access or take actions beyond those expected or intended.

b) Counting Rules

- Severe vulnerabilities identified across the enterprise during the time period

c) Counting Rule Exclusions

- Vulnerabilities supplier rated as severe but organizationally ranked lower should be validated before exclusion.

d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
PSWKSV	Percent of Systems Without Known Severe Vulnerabilities	Count (Systems_Without_Known_Severe_Vulnerabilities)*100/ Count(Scanned_Systems)	Percentage of systems

1.4.5 Sources of Data

Vulnerability management systems will provide information on which systems were identified with severe vulnerabilities.

1.4.6 Reporting Frequency

Weekly is recommended but can be reported Monthly, Quarterly or Annually

1.4.7 Source of Measurement

CIS

1.4 既知の深刻な脆弱性がないシステムの比率

1.4.1 一般

既知の深刻な脆弱性がないシステムの比率（PSWKSV）は，脆弱性スキャンにおいていかなる既知の深刻な脆弱性も発見されなかったシステムの比率を測定する。

脆弱性管理は，新たな深刻な脆弱性の識別及び既知の深刻な脆弱性の改善の両方を含むので，既知の深刻な脆弱性がないシステムの比率（PSWKSV）は時間とともに変化する。組織は，この測定を悪用にさらされる相対的なレベルの測定に使用することができ，セキュリティインシデント（ひいては組織上への影響）についての予想レベルの潜在的な指標となる。

組織のリスクプロファイルには必ずしも重要でない，検出される多数の情報，局所的な，セキュリティ上の弱点となる脆弱性があるので，この重大さのしきい値は重要である。管理者は一般に，最初に，より大きなリスクに焦点をあてるために，不要な情報のレベルを減らそうとするであろう。この測定はビジネスユニットの資産重要度などに応じて，システムのサブセットについても計算できる。

1.4.2 目的

既知の深刻な脆弱性がないシステムの比率（PSWKSV）は，組織が既知の深刻な脆弱性にさらされる相対的な比率を測定する。測定は，いかなる既知の深刻な脆弱性も持っていないとスキャンされたシステムの比率を評価する。

1.4.3 適用する製品分類

コアネットワーク製品及びエンドユーザサービス。製品分類表の最新版は
http://tl9000.org/resources/resources.html を参照。

1.4.4 詳細説明

a) 用語

脆弱性 ― 脆弱性とは，攻撃者による予期又は意図しないアクセス又は行動によって悪用される可能性のある弱点と定義される。

b) 計数ルール

期間中に企業全体で認識された深刻な脆弱性

c) 計数ルールの除外

供給者が深刻と評価したが，組織的にはより低く評価された脆弱性は，除外する前に検証されることが望ましい。

d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
PSWKSV	既知の深刻な脆弱性がないシステムの比率	既知の深刻な脆弱性のないシステム数／スキャンしたシステム数＊100	システムの比率

1.4.5 データ発生源

脆弱性管理システムは，どのシステムで深刻な脆弱性が検出されたかの情報を提供する。

1.4.6 報告頻度

週次を推奨するが，月次，四半期又は年次報告でも良い

1.4.7 測定法出典

CIS

1.5 Mean-Time to Mitigate Vulnerabilities

1.5.1 General Description and Title

Mean-Time to Mitigate Vulnerabilities measures the average time taken to mitigate vulnerabilities identified in an organization's technologies. The vulnerability management processes consists of the identification and remediation of known vulnerabilities in an organization's environment. This metric is an indicator of the performance of the organization in addressing identified vulnerabilities. The less time required to mitigate vulnerability the more likely an organization can react effectively to reduce the risk of exploitation of vulnerabilities.

It is important to note that only data from vulnerabilities explicitly mitigated are included in this metric result. The metric result is the mean time to mitigate vulnerabilities that are actively addressed during the metric time period, and not a mean time to mitigate based on the time for all known vulnerabilities to be mitigated.

1.5.2 Purpose

Mean-Time to Mitigate Vulnerabilities (MTTMV) measures the average amount of time required to mitigate an identified vulnerability. This metric indicates the performance of the organization in reacting to vulnerabilities identified in the environment. It only measures the time average times for explicitly mitigated vulnerabilities, and not mean time to mitigate any vulnerability, or account for vulnerabilities that no longer appear in scanning activities.

1.5.3 Applicable Categories

Core Network Products and End Customer Services. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

1.5.4 Detailed Description

a) Terminology
Vulnerability -- Vulnerability is defined as a weakness that could be exploited by an attacker to gain access or take actions beyond those expected or intended.

b) Counting Rules
- All vulnerabilities identified across the enterprise during the time period

c) Counting Rule Exclusions
- None

d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
MTTMV	Mean-Time to Mitigate Vulnerabilities	Sigma (Date_of_Mitigation - Date_of_Detection)/ Count(Mitigated_Vulnerabilities)	Hours per vulnerability

1.5.5 Sources of Data

Vulnerability management systems will provide information on which systems were identified with severe vulnerabilities.

1.5.6 Reporting Frequency

Weekly is recommended but can be reported Monthly, Quarterly or Annually

1.5.7 Source of Measurement

CIS

1.5 平均脆弱性軽減時間

1.5.1 一般

平均脆弱性軽減時間は，組織の技術部門で確認された脆弱性を軽減するために費やされた時間の平均値を測定する。脆弱性管理プロセスは，組織の環境内における既知の脆弱性を確認すること，及びそれを軽減することからなっている。この測定値は，既知の脆弱性に言及する際の，組織のパフォーマンスの指標である。脆弱性を軽減するのに要する時間が短ければ短いほど，組織が脆弱性を悪用されるリスクを軽減するよう効果的に対処することのできる度合いが高くなる。
重要なことは，脆弱性から明白に軽減されたデータのみがこの測定結果に含まれるということに注意すべきである。この測定結果は，測定期間において，積極的に対処がなされている脆弱性を軽減するための平均時間であり，全ての既知の脆弱性を軽減するのに要する時間をもとにした平均軽減時間ではない。

1.5.2 目的

平均脆弱性軽減時間(MTTMV)は，確認された単独の脆弱性を軽減するのに要する平均時間量を測定する。この測定値は，組織の環境内で確認された脆弱性に対応する組織のパフォーマンスを示している。これは，脆弱性を明白に軽減するために要した平均時間のみを測定するのであって，全ての脆弱性を軽減するために必要な平均時間ではなく，また調査しても 2 度と出現しないような脆弱性は計算に入れない。

1.5.3 適用する製品分類

コアネットワーク製品及びエンドユーザサービス。製品分類表の最新版は
http://tl9000.org/resources/resources.html を参照。

1.5.4 詳細説明

a) 用語
脆弱性 －脆弱性とは，攻撃者による予期又は意図しないアクセス又は行動によって悪用される可能性のある弱点と定義される。

b) 計数ルール
- 一定期間に企業全体に亘って確認された全ての脆弱性

c) 計数ルールの除外
- なし

d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
MTTMV	平均脆弱性軽減時間	Σ (軽減した日 - 検出した日) /軽減された脆弱性の数	脆弱性当たりの時間

1.5.5 データ発生源

脆弱性管理システムは，どのシステムで深刻な脆弱性が検出されたかの情報を提供する。

1.5.6 報告頻度

週次を推奨するが，月次，四半期又は年次報告でも良い。

1.5.7 測定法出典

CIS

1.6 Patch Policy Compliance

1.6.1 General Description and Title

Patch Policy Compliance (PPC) measures an organization's patch level for supported technologies as compared to their documented patch policy.

"Policy" refers to the patching policy of the organization, more specifically, which patches are required for what type of computer systems at any given time. This policy might be as simple as "install the latest patches from system vendors" or may be more complex to account for the criticality of the patch or system.

"Patched to policy" reflects an organization's risk/reward decisions regarding patch management. It is not meant to imply that all vendor patches are immediately installed when they are distributed.

1.6.2 Purpose

Patch Policy Compliance (PPC) indicates the scope of the organization's patch level for supported technologies as compared to their documented patch policy. While specific patch policies may vary within and across organizations, performance versus stated patch state objectives can be compared as a percentage of compliant systems.

1.6.3 Applicable Categories

Core Network Products and End Customer Services. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

1.6.4 Detailed Description

a) Terminology

Security Patch -- A patch is a modification to existing software in order to improve functionality, fix bugs, or address security vulnerabilities. Security patches are patches that are solely or in part created and released to address one or more security flaws, such as, but not limited to publicly disclosed vulnerabilities.

b) Counting Rules

None

c) Counting Rule Exclusions

None

d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
PPC	Patch Policy Compliance	Count(Compliant_Instances)*100 / Count(Technology_Instances)	Percentage of technology instances

1.6.5 Sources of Data

Patch management and IT support tracking systems will provide patch deployment data. Audit reports will provide compliance status.

1.6.6 Reporting Frequency

Weekly is recommended but can be reported Monthly, Quarterly or Annually

1.6.7 Source of Measurement

CIS

1.6 パッチ方針適合性

1.6.1 一般

パッチ方針適合性（PPC）は，組織の文書化されたパッチ方針と比較することで，サポートされた技術に対するに組織のパッチレベルを測定する。

"方針"とは，組織のパッチ方針であり，具体的には，常にどの種類のコンピュータシステムにどのパッチが必要かを示す。この方針は，「システムベンダーから最新のパッチをインストールする」のと同じくらい単純かもしれないが，パッチ又はシステムの重大性のために，より複雑になる場合がある。

「パッチ化の方針」は，パッチマネジメントに関して組織のリスク／報酬の決定を反映する。すべてのベンダーのパッチが配布されるとき，それらがすぐにインストールされることを意味しない。

1.6.2 目的

パッチ方針適合性（PPC）は，組織の文書化されたパッチ方針と比較することで，サポートされた技術のために組織のパッチレベルの範囲を示す。具体的なパッチ方針は，組織の内部及び組織を超えて様々であるが，規定したパッチ状況目標に対するパフォーマンスは，システムの適合率として比較できる。

1.6.3 適用する製品分類

コアネットワーク製品及びエンドユーザサービス。製品分類表の最新版は
http://tl9000.org/resources/resources.html を参照。

1.6.4 詳細説明

a) 用語

セキュリティパッチーパッチは，機能向上，バグ修正，又はセキュリティ脆弱性への対処のために既存のソフトウェアを変更するものである。セキュリティパッチは，単独のパッチとして，又はパッチの一部として作成，リリースされ，１つ又は複数のセキュリティの欠陥，例えば，公開された脆弱性（これに限られるわけではない），に対処するものである。

b) 計数ルール

なし

c) 計数ルールの除外

なし

d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
PPC	パッチ方針適合性	適合するインスタンス数*100 / 技術的インスタンス数	技術的インスタンス数の比率

1.6.5 データ発生源

パッチマネジメントと IT サポート追跡システムは，パッチの展開データを提供する。 監査報告書は，適合性の状態を提供する。

1.6.6 報告頻度

週次を推奨するが，月次，四半期又は年次報告でも良い

1.6.7 測定法出典

CIS

1.7 Mean Time to Patch

1.7.1 General Description and Title

Mean Time to Patch (MTTP) measures the average time taken to deploy a patch to the organization's technologies. The more quickly patches can be deployed, the lower the mean time to patch and the less time the organization spends with systems in a state known to be vulnerable.

1.7.2 Purpose

Mean Time to Patch (MTTP) characterizes the effectiveness of the patch management process by measuring the average time taken from date of patch release to installation in the organization for patches deployed during the metric time period. This metric serves as an indicator of the organization's overall level of exposure to vulnerabilities by measuring the time the organization takes to address systems known to be in vulnerable states that can be remediated by security patches. This is a partial indicator as vulnerabilities may have no patches available or occur for other reasons such as system configurations.

1.7.3 Applicable Categories

Core Network Products and End Customer Services. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

1.7.4 Detailed Description

a) Terminology

Security Patch -- A patch is a modification to existing software in order to improve functionality, fix bugs, or address security vulnerabilities. Security patches are patches that are solely or in part created and released to address one or more security flaws, such as, but not limited to publicly disclosed vulnerabilities.

b) Counting Rules

None

c) Counting Rule Exclusions

None

d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
MTTP	Mean Time to Patch	Sigma(Date_of_Installation - Date_of_Availability) / Count(Completed_Patches)	Hours per patch

1.7.5 Sources of Data

Patch management and IT support tracking systems will provide patch deployment data.

1.7.6 Reporting Frequency

Weekly is recommended but can be reported Monthly, Quarterly or Annually

1.7.7 Source of Measurement

CIS

1.7 平均パッチ時間

1.7.1 一般

平均パッチ時間(MTTP)は，組織の技術設備に対しパッチを展開するために要した平均時間を測定する。より迅速にパッチを展開できれば，より平均パッチ時間が短くなり，組織のシステムが脆弱な状態に留まる時間がより短くなる。

1.7.2 目的

平均パッチ時間（MTTP）は，期間内に展開されたパッチに対してパッチリリースの日から組織でインストールにかかった平均時間の測定によってパッチ管理プロセスの有効性を示す。この測定は，セキュリティパッチによって修正することができる脆弱な状態と分かっているシステムを，組織が対処するための時間を測定することによって，組織全体での脆弱性にさらされるレベルの指標として役立つ。これは，利用可能なパッチがないか，システム構成のような他の理由で起こるかもしれない脆弱性には，部分的な指標である。

1.7.3 適用する製品分類

コアネットワーク製品及びエンドユーザサービス。製品分類表の最新版は http://tl9000.org/resources/resources.html を参照。

1.7.4 詳細説明

a) 用語

セキュリティパッチーパッチは，機能向上，バグ修正，又はセキュリティ脆弱性への対処のために既存のソフトウェアを変更するものである。セキュリティパッチは，単独のパッチとして，又はパッチの一部として作成，リリースされ，１つ又は複数のセキュリティの欠陥，例えば公開された脆弱性（これに限られるわけではない）に対処するものである。

b) 計数ルール

なし

c) 計数ルールの除外

なし

d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
MTTP	平均パッチ時間	Σ(インストールの日– 入手可能な日) / 完了したパッチ数	パッチ当たりの時間

1.7.5 データ発生源

パッチマネジメントと IT サポート追跡システムは，パッチの展開データを提供する。

1.7.6 報告頻度

週次を推奨するが，月次，四半期又は年次報告でも良い

1.7.7 測定法出典

CIS

1.8 Percentage of Configuration Compliance

1.8.1 General Description and Title

The Percent of Configuration Compliance (PCC) measures the effectiveness of configuration management in the context of information security. A percentage metric will allow benchmarking across organizations.

1.8.2 Purpose

The goal of this metric is to provide an indicator of the effectiveness of an organization's configuration management policy relative to information security, especially emerging exploits. If 100% of systems are configured to standard, then those systems are relatively more secure and manageable. If this metric is less than 100%, then those systems are relatively more exposed to exploits and to unknown threats.

1.8.3 Applicable Categories

Core Network Products and End Customer Services. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

1.8.4 Detailed Description

a) Terminology
   None
b) Counting Rules
   None
c) Counting Rule Exclusions
   None
d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
PCC	Percentage of Configuration Compliance	Sigma(In Scope Systems With Approved Configuration) *100/ Count(In Scope Systems)	Percentage of Systems

1.8.5 Sources of Data

Configuration management and IT support tracking system audit reports will provide compliance status. Automated testing tools for CIS benchmarks are also available.

1.8.6 Reporting Frequency

Monthly

1.8.7 Source of Measurement

CIS

1.8 構成適合性比率

1.8.1 一般

構成適合性比率（PCC）は，構成管理の効果を情報セキュリティの面で測定する。比率の測定方法は，組織全体のベンチマークを可能とする。

1.8.2 目的

この測定の目的は，情報セキュリティ，特に新たな悪用，に対する組織の構成管理方針の有効性を示す指標を提供することにある。もし，この測定が１００％未満ならば，それらのシステムは，悪用及び未知の脅威に比較的さらされ易い。

1.8.3 適用する製品分類

コアネットワーク製品及びエンドユーザサービス。製品分類表の最新版は http://tl9000.org/resources/resources.html を参照。

1.8.4 詳細説明

a) 用語
   なし
b) 計数ルール
   なし
c) 計数ルールの除外
   なし
d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
PCC	構成適合性比率	Σ(承認された構成により適用されるシステム)*100/ 適用されるシステム数	システムの比率

1.8.5 データ発生源

構成管理と IT サポート追跡システム監査報告書は適合性の状態を提供する。CIS ベンチマークのための自動試験ツールも利用可能である。

1.8.6 報告頻度

毎月

1.8.7 測定法出典

CIS

1.9 Mean Time to Complete Changes

1.9.1 General Description and Title
The average time it takes to complete a configuration change request.

1.9.2 Purpose
The goal of this metric is to provide managers with information on the average time it takes for a configuration change request to be completed.

1.9.3 Applicable Categories
Core Network Products and End Customer Services. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

1.9.4 Detailed Description
a) Terminology
None
b) Counting Rules
None
c) Counting Rule Exclusions
None
d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
MTCC	Mean Time to Complete Changes	Sigma(Completion_Date - Submission_Date) / Count(Completed_Changes)	Days per configuration change request

1.9.5 Sources of Data
Configuration management and IT support tracking systems will provide configuration change data.

1.9.6 Reporting Frequency
Weekly is recommended but can be reported Monthly, Quarterly or Annually

1.9.7 Source of Measurement
CIS

1.9 平均変更完了時間

1.9.1 一般
構成変更要求が完了するまでに要する平均時間。
1.9.2 目的
この測定の目的は，構成変更要求が完了するまでにかかる平均時間に関する情報を管理者に提供することにある。

1.9.3 適用する製品分類
コアネットワーク製品及びエンドユーザサービス。製品分類表の最新版は
http://tl9000.org/resources/resources.html を参照。

1.9.4 詳細説明
a) 用語
なし
b) 計数ルール
なし
c) 計数ルールの例外
なし
d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
MTCC	平均変更完了時間	Σ(完了日－提出日)/完了した変更数	構成変更要求ごとの日数

1.9.5 データ発生源
構成管理と IT サポート追跡システムは構成変更データを提供する。

1.9.6 報告頻度
週次を推奨するが，月次，四半期又は年次報告でも良い
1.9.7 測定法出典
CIS

1.10 Percent of Changes with Security Review

1.10.1 General Description and Title
This metric indicates the percentage of configuration or system changes that were reviewed for security impacts before the change was implemented.

1.10.2 Purpose
The goal of this metric is to provide managers with information about the amount of changes and system churn in their environment that have unknown impact on their security state.

1.10.3 Applicable Categories
Core Network Products and End Customer Services. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

1.10.4 Detailed Description
a) Terminology
None
b) Counting Rules
Only completed changes should apply.
c) Counting Rule Exclusions
None
d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
PCSR	Percent of Changes with Security Review	Sigma(Completed_Changes_with_Security_Reviews)*100/ Count(Completed_Changes)	Percentage of configuration changes

1.10.5 Sources of Data
Configuration management and IT support tracking systems will provide configuration change data.

1.10.6 Reporting Frequency
Weekly is recommended but can be reported Monthly, Quarterly or Annually

1.10.7 Source of Measurement
CIS

1.10 セキュリティレビュー変更比率

1.10.1 一般
この測定は，変更が実施される前にセキュリティへの影響をレビューされた構成変更又はシステム変更の比率を表す。

1.10.2 目的
この測定の目的は，セキュリティ状況に未知の影響を及ぼすような，組織環境での変更及びシステムチャーン（churn）の量に関する情報を管理者に提供することである。

1.10.3 適用する製品分類
コアネットワーク製品及びエンドユーザサービス。製品分類表の最新版は，
http://tl9000.org/resources/resources.html.を参照。

1.10.4 詳細説明
a) 用語
なし
b) 計数ルール
完了した変更のみに適用する。
c) 計数ルールの除外
なし
d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
PCSR	セキュリティレビュー変更比率	Σ（完了したセキュリティレビュー変更件数）*100 / 完了した変更件数	構成変更の比率

1.10.5 データ発生源
構成管理と IT サポート追跡システムは構成変更データを提供する。

1.10.6 報告頻度
週次を推奨するが，月次，四半期又は年次報告でも良い

1.10.7 測定法出典
CIS

1.11 Percent of Changes with Security Exceptions

1.11.1 General Description and Title
This metric indicates the percentage of configuration or system changes that received an exception to existing security policy.

1.11.2 Purpose
The goal of this metric is to provide managers with information about the potential risks to their environment resulting from configuration or system changes exempt from the organization's security policy.

1.11.3 Applicable Categories
Core Network Products and End Customer Services. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

1.11.4 Detailed Description
a) Terminology
None
b) Counting Rules
Only completed changes should apply.
Security exceptions may only have been granted for systems that have received security reviews.
c) Counting Rule Exclusions
None
d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
PCSE	Percent of Changes with Security Exception	Sigma(Completed_Changes_with_Security_Exceptions)*100/ Count(Completed_Changes)	Percentage of configuration changes

1.11.5 Sources of Data
Configuration management and IT support tracking systems will provide configuration change data.

1.11.6 Reporting Frequency
Weekly is recommended but can be reported Monthly, Quarterly or Annually

1.11.7 Source of Measurement
CIS

1.11 セキュリティ除外変更比率

1.11.1 一般
この測定は，既存のセキュリティ方針の適用除外を受けた構成変更又はシステム変更の比率を表す。
1.11.2 目的
この測定の目的は，組織のセキュリティ方針から免除された構成変更又はシステム変更に起因する組織環境の潜在的なリスクに関する情報を管理者に提供することである。

1.11.3 適用する製品分類
コアネットワーク製品及びエンドユーザサービス。製品分類表の最新版は，
http://tl9000.org/resources/resources.html.を参照。

1.11.4 詳細説明
a) 用語
なし
b) 計数ルール
完了した変更のみに適用する。
セキュリティの除外は，セキュリティレビューを受けたシステムにのみ与えてもよい。
c) 計数ルールの除外
なし
d))計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
PCSE	セキュリティ除外変更比率	Σ（完了したセキュリティ除外の変更件数）*100 / 完了した変更件数	構成変更の比率

1.11.5 データ発生源
構成管理及び IT サポート追跡システムは構成変更データを提供する。

1.11.6 報告頻度
週次を推奨するが，月次，四半期又は年次報告でも良い

1.11.7 測定法出典
CIS

1.12 Risk Assessment Coverage

1.12.1 General Description and Title
Risk assessment coverage indicates the percentage of business applications that have been subject to a risk assessment at any time.

1.12.2 Purpose
This metric reports the percentage of applications that have been subjected to risk assessments.

1.12.3 Applicable Categories
Core Network Products and End Customer Services. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

1.12.4 Detailed Description
a) Terminology

Risk Assessment -- The term risk assessment is defined as a process for analyzing a system and identifying the risks from potential threats and vulnerabilities to the information assets or capabilities of the system. Although many methodologies can be used, it should consider threats to the target systems, potential vulnerabilities of the systems, and impact of system exploitation. It may or may not include risk mitigation strategies and countermeasures.

b) Counting Rules

None

c) Counting Rule Exclusions

None

d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
RAC	Risk Assessment Coverage	Count(Applications_Undergone_Risk_Assessment)*100/ Count(Applications)	Percent of applications

1.12.5 Sources of Data
The data source for this metric is a risk assessment tracking system.

1.12.6 Reporting Frequency
Weekly is recommended but can be reported Monthly, Quarterly or Annually

1.12.7 Source of Measurement
CIS

1.12 リスクアセスメント適用率

1.12.1 一般
リスクアセスメント適用率は，常に，リスクアセスメントの対象となった業務アプリケーションの比率を示す。

1.12.2 目的
この測定は，リスクアセスメントの対象となったアプリケーションの比率を報告する。

1.12.3 適用する製品分類
コアネットワーク製品及びエンドユーザサービス。製品分類表の最新版は，
http://tl9000.org/resources/resources.html を参照。

1.12.4 詳細説明
a) 用語

リスクアセスメント―リスクアセスメントとは，システムを分析し，潜在的脅威及び脆弱性が情報資産又はシステムの機能に与えるリスクを特定するプロセスであると定義される。多くの手法を使用できるが，ターゲットシステムへの脅威，潜在的なシステムの脆弱性，及びシステム悪用の影響を考慮することが望ましい。リスク軽減のための戦略及び対応を含んでいなくてもよい。

b) 計数ルール

なし

c) 計数ルールの除外

なし

d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
RAC	リスクアセスメント適用率	リスクアセスメントを受けたアプリケーション数×100/アプリケーション数	アプリケーションの比率

1.12.5 データ発生源
この測定法のデータ発生源は，リスクアセスメント追跡システムである。

1.12.6 報告頻度
週次を推奨するが，月次，四半期又は年次報告でも良い

1.12.7 測定法出典
CIS。

1.13 Security Testing Coverage

1.13.1 General Description and Title

This metric tracks the percentage of applications in the organization that have been subjected to security testing. Testing can consists of manual or automated white and/or black-box testing and generally is performed on systems post-deployment (although they could be in pre-production testing).

1.13.2 Purpose

This metric indicates the percentage of the organization's applications have been tested for security risks.

1.13.3 Applicable Categories

Core Network Products and End Customer Services. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

1.13.4 Detailed Description

a) Terminology

None

b) Counting Rules

Methodology for counting applications – Refer to CIS Security Metrics document v1.0, section titled Application Security Metrics.

c) Counting Rule Exclusions

None

d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
STC	Security Testing Coverage	Count(Applications_Undergone_Security_Testing)*100/ Count(Deployed_Applications)	Percent of applications

1.13.5 Sources of Data

TBD

1.13.6 Reporting Frequency

Weekly is recommended but can be reported Monthly, Quarterly or Annually

1.13.7 Source of Measurement

CIS

1.13 セキュリティ試験適用率

1.13.1 一般

この測定は，セキュリティ試験の対象となった組織内のアプリケーションの比率を追跡する。試験には，手動又は自動のホワイト及び/又はブラックボックス試験があり，（生産前試験で実施することも可能であるが）一般に展開後のシステムで実施される。

1.13.2 目的

この測定法は，セキュリティリスクに対する試験を実施された組織内のアプリケーションの比率を示す。

1.13.3 適用する製品分類

コアネットワーク製品及びエンドユーザサービス。製品分類表の最新版は，
http://tl9000.org/resources/resources.html を参照。

1.13.4 詳細説明

a) 用語

なし

b) 計数ルール

アプリケーションの計数方法—CIS のセキュリティ測定法文書 バージョン 1.0 の「アプリケーションのセキュリティ測定法」のセクションを参照。

c) 計数ルールの除外

なし

d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
STC	セキュリティ試験適用率	セキュリティ試験を受けたアプリケーションの比率 アプリケーション数×100/展開されたアプリケーション数	

1.13.5 データ発生源

未確定。

1.13.6 報告頻度

週次を推奨するが，月次，四半期又は年次報告でも良い

1.13.7 測定法出典

CIS。

2.1 Vulnerability Measure

2.1.1 General Description and Title

Vulnerability Measure measures the percentage of high vulnerabilities mitigated within the organizationally defined time periods after discovery.

2.1.2 Purpose

Ensure an environment of comprehensive security and accountability for personnel, facilities, and products. Ensure all vulnerabilities are identified and mitigated.

2.1.3 Applicable Product Categories

Core Network Products and End Customer Services. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

2.1.4 Detailed Description

a) Terminology
Vulnerability -- Vulnerability is defined as a weakness that could be exploited by an attacker to gain access or take actions beyond those expected or intended.

b) Counting Rules
- High vulnerabilities identified across the enterprise during the time period
- High vulnerabilities mitigated across the enterprise during the time period

c) Counting Rule Exclusions
- Vulnerabilities supplier rated as high but organizationally ranked lower with no mitigation should be validated before exclusion.

d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
VM	Vulnerability Measure	(number of high vulnerabilities mitigated within targeted time frame) / (number of high vulnerabilities identified during time frame)	% of vulnerabilities mitigated should be a high target set by the organization.

2.1.5 Sources of Data

Vulnerability scanning software, audit logs, vulnerability management systems, patch management systems, change management records.

2.1.6 Reporting Frequency

Organization defined (example annually)

2.1.7 Source of Measurement

NIST – SP800-53, RA-5

2.1 脆弱性測定

2.1.1 一般

脆弱性測定は，発見後，組織が定義した期間内に軽減された高脆弱性の比率を測定する。

2.1.2 目的

要員，設備及び製品に対する包括的なセキュリティ環境及びアカウンタビリティを確実にする。すべての脆弱性の特定及び軽減を確実にする。

2.1.3 適用する製品分類

コアネットワーク製品及びエンドユーザサービス。製品分類表の最新版は，
http://tl9000.org/resources/resources.html を参照。

2.1.4 詳細説明

a) 用語
脆弱性—脆弱性とは，攻撃者による予期又は意図しないアクセス又は行動によって悪用される可能性のある弱点と定義される。

b) 計数ルール
- 一定期間内に企業全体で特定された高脆弱性
- 一定期間内に企業全体で軽減された高脆弱性

c) 計数ルールの除外
- 供給者が高く評価したが，組織的には軽減なしで低く評価された脆弱性は，除外する前に有効性を確認することが望ましい。

d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
VM	脆弱性測定	目標期間内に軽減された高脆弱性の数/期間内に確認された高脆弱性の数	軽減された脆弱性の比率は，組織によって設定された高い目標値であることが望ましい。

2.1.5 データ発生源

脆弱性スキャンソフトウェア，監査ログ，脆弱性管理システム，パッチ管理システム，変更管理記録。

2.1.6 報告頻度

組織が定める（例：毎年）

2.1.7 測定法出典

NIST‐SP800-53，RA-5。
[訳注：NIST; National Institute of Standards and Technology 「米国国立標準技術研究所」の略 ST800-53 Recommended Security Controls for Federal Information Systems 「連邦政府情報システムにおける推奨セキュリティ管理策」]

2.2 Remote Access Control Measure

2.2.1 General Description and Title

Remote Access Control Measure measures the percentage of remote access points used to gain unauthorized access.

2.2.2 Purpose

Ensure an environment of comprehensive security and accountability for personnel, facilities, and products. Restrict information, systems, and component access to individuals or machines that are identifiable, known, credible, and authorized.

2.2.3 Applicable Product Categories

End Customer Services. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

2.2.4 Detailed Description

a) Terminology
Remote Access – Refer to NIST – SP800-53, AC-17

b) Counting Rules

- Remote access points for the organization
- Access points used to gain unauthorized access based on incident logs, IDS, and remote access logs

c) Counting Rule Exclusions

- Invalid exclusions will result if the organization does not document all remote access points (CM-2), use Intrusion Detection Systems to monitor remote access points (SI-4), collect/review remote access audit logs (AU-6), and normalize incident categories for security incidents (IR-5)

d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
RACM	Remote Access Control Measure	(Number of remote access points used to gain unauthorized access) / (total number of remote access points)	% of successful unauthorized accesses should be a very low number set by the organization.

2.2.5 Sources of Data

Incident database, audit logs, network diagrams, IDS logs and alerts

2.2.6 Reporting Frequency

Organization defined (example: quarterly)

2.2.7 Source of Measurement

NIST – SP800-53, AC-17

2.2 リモートアクセス制御測定

2.2.1 一般

リモートアクセス制御測定は，不正アクセスに使用されたリモートアクセスポイントの比率を測定する。

2.2.2 目的

要員，設備及び製品に対する包括的なセキュリティ環境及びアカウンタビリティを確実にする。情報，システム及びコンポーネントへのアクセスを特定可能で，既知で，信頼でき，及び権限を与えられた個人又は装置に制限する。

2.2.3 適用する製品分類

エンドユーザサービス。製品分類表の最新版は，http://tl9000.org/resources/resources.html を参照。

2.2.4 詳細説明

a) 用語
リモートアクセス — NIST - SP800-53，AC-17 を参照。

b) 計数ルール

- 組織のリモートアクセスポイント
- インシデントログ，IDS 及びリモートアクセスログに基づく，不正アクセスに使用されたアクセスポイント

c) 計数ルールの除外

- 組織がすべてのリモートアクセスポイントを文書化していない（CM-2），リモートアクセスポイントを監視する侵入検知システムを使用していない（SI-4），リモートアクセス監査ログを収集/レビューしていない（AU-6），及びセキュリティインシデントのインシデント分類を規準化していない（IR-5）場合，除外は無効となる。

d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
RACM	リモートアクセス制御測定	不正アクセスに使用されたリモートアクセスポイントの数/リモートアクセスポイントの合計数	不正アクセスが成功した比率は，組織によって設定された非常に低い数値であることが望ましい。

2.2.5 データ発生源

インシデントデータベース，監査ログ，ネットワーク図，IDS ログ，及び警報。

2.2.6 報告頻度

組織が定める（例：四半期毎）

2.2.7 測定法出典

NIST - SP800-53，AC-17。

2.3 Security Training Measure

2.3.1 General Description and Title

Security Training Measure measures the percentage of information system security personnel that have received security training.

2.3.2 Purpose

Ensure a high-quality work force supported by modern and secure infrastructure and operational capabilities. Ensure that organization personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

2.3.3 Applicable Categories

All Product Categories. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

2.3.4 Detailed Description

a) Terminology

None

b) Counting Rules

- Employees in the organization having significant security responsibilities
- Employees with significant security responsibilities that have received required training

c) Counting Rule Exclusions

- Invalid exclusions will result if the organization does not formally identify employees with significant security responsibilities (AT-3) or maintain adequate training records (AT-4)

d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
STM	Security Training Measure	(Number of information system security personnel completing security training in the past year) / (total number of information system security personnel)	% of security personnel completing required training in a year should be a high number set by the organization.

2.3.5 Sources of Data

Training awareness and tracking records

2.3.6 Reporting Frequency

Organization defined (example: annually)

2.3.7 Source of Measurement

NIST – SP800-53, AT-3

2.3 セキュリティ教育・訓練測定

2.3.1 一般

セキュリティ教育・訓練測定は，セキュリティ教育・訓練を受けた情報システムセキュリティ要員の比率を測定する。

2.3.2 目的

最新で安全なインフラストラクチャー及び運用能力に支えられた高品質な労働力を確実にする。組織の要員が，割り当てられた情報セキュリティ関連の職務及び責任を実行するのに十分な教育・訓練がされていることを確実にする。

2.3.3 適用する製品分類

全ての製品分類。製品分類表の最新版は，

http://tl9000.org/resources/resources.html を参照。

2.3.4 詳細説明

a) 用語

なし

b) 計数ルール

- 組織内で重要なセキュリティ責任を持つ要員
- 重要なセキュリティ責任を持ち，必要な教育・訓練を受けた要員

c) 計数ルールの除外

- 組織が重要なセキュリティ責任を持つ要員を正式に特定していない（AT-3），又は十分な教育・訓練記録を維持していない（AT-4）場合，除外は無効となる。

d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
STM	セキュリティ教育・訓練測定	過去 1 年以内にセキュリティ教育・訓練を完了した，情報システムセキュリティ要員の数/情報システムセキュリティ要員の合計数	1 年以内に必要な訓練を完了したセキュリティ要員の比率は，組織によって設定された高い数値であることが望ましい。

2.3.5 データ発生源

教育・訓練に対する認識及び受講記録。

2.3.6 報告頻度

組織が定める（例：毎年）

2.3.7 測定法出典

NIST – SP800-53，AT-3。

2.4 Audit Record Review Measure

2.4.1 General Description and Title

Audit Record Review Measure measures the average frequency of audit records review and analysis for inappropriate activity.

2.4.2 Purpose

Ensure an environment of comprehensive security and accountability for personnel, facilities, and products. Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate activity.

2.4.3 Applicable Categories

All Product Categories. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

2.4.4 Detailed Description

a) Terminology
Audit Record -- Any log or record related to security such as a security log for a product or access log (physical building or product).

b) Counting Rules

- System audit logs reviewed within the following time periods: past day, past week, 2 weeks to 1 month, 1 month to 6 months, over 6 months
- For Collection Frequency, refer to NIST – SP800-53, AU-6.

c) Counting Rule Exclusions

- Invalid exclusions will result for systems not adequately logging system data (AU-2) and for activities inappropriately categorized within system logs.

d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
ARRM	Audit Record Review Measure	Average frequency during reporting time.	Average frequency of log reviews during the time period should be a high frequency set by the organization.

2.4.5 Sources of Data

Audit log reports

2.4.6 Reporting Frequency

Organization defined (example: quarterly)

2.4.7 Source of Measurement

NIST – SP800-53, AU-6

2.4 監査記録レビュー測定

2.4.1 一般

監査記録レビュー測定は，不適切な活動に対する監査記録のレビュー及び分析の平均頻度を測定する。

2.4.2 目的

要員，設備及び製品に対する包括的なセキュリティ環境及びアカウンタビリティを確実にする。非合法，無許可，又は不適切な活動の監視，分析，調査と報告を可能にするために，必要な範囲で情報システム監査記録を作成，保護，保管する。

2.4.3 適用する製品分類

全ての製品分類。製品分類表の最新版は
http://tl9000.org/resources/resources.html を参照。を参照。

2.4.4 詳細説明

a) 用語
監査記録―ある製品のセキュリティログや（物理的な建物や製品への）アクセスログのようなセキュリティと関連するログ，また記録を意味する。

b) 計数ルール

- 以下の期間内にシステム監査ログのレビューが実施される：前日，先週，2 週間～1 ヶ月，1 ヶ月～6 ヶ月，6 ヶ月以上。
- 収集頻度 について，NIST – SP800-53, AU-6 を参照。

c) 計数ルールの除外
システムがシステムデータ（AU-2）を適切に記録しない場合，及び活動がシステムログのなかで不適切に分類されている場合，除外は無効となる。

d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
ARRM	監査記録レビュー測定	報告期間における平均頻度	期間内のログレビューの平均頻度は組織によって設定された高頻度であることが望ましい。

2.4.5 データ発生源

監査ログレポート

2.4.6 報告頻度

組織が定める（例：四半期毎）

2.4.7 測定法出典

NIST – SP800-53, AU-6

2.5 C&A Completion Measure

2.5.1 General Description and Title

C&A Compliance Measure measures the percentage of new systems that have completed certification and accreditation (C&A) prior to their implementation.

2.5.2 Purpose

Ensure an environment of comprehensive security and accountability for personnel, facilities, and products. Ensure all information systems have been certified and accredited as required.

2.5.3 Applicable Categories

End Customers Services. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

2.5.4 Detailed Description

a) Terminology
   - C&A – Certification, Accreditation, and Security Assessments performed per the organization's internal requirements
   - Authorizing Official [AO] – Group or individual with the authority to formally certify a system for implementation

b) Counting Rules
   - Number of new systems implemented during the reporting time period
   - Number of new systems implemented during the reporting time period that received authority to operate prior to implementation

c) Counting Rule Exclusions
   - Invalid exclusions will result for organizations that do not maintain a system inventory, implement a formal C&A process (CA-1), or require all systems to complete the C&A process prior to implementation.

d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
CACM	C&A Completion Measure	(number of new systems with complete C&A packages with AO approval prior to implementation) / (total number of newly implemented systems)	% of new systems certified prior to implementation should be a high number set by the organization

2.5.5 Sources of Data

System inventory, system C&A documentation

2.5.6 Reporting Frequency

Organization defined (example: annually)

2.5.7 Source of Measurement

NIST – SP800-53, CA-6

2.5 認証及び認定（C&A）完了測定

2.5.1 一般

C&A 完了測定は，システム導入前に認証及び認定（C&A）を完了した新規システムの比率を測定する。

2.5.2 目的

設備及び製品に対する包括的なセキュリティ環境及びアカウンタビリティを確実にする。すべての情報システムが要求どおり認証及び認定されていることを確実にする。

2.5.3 適用する製品分類

エンドユーザサービス。製品分類の最新版は

http://tl9000.org/resources/resources.html を参照。

2.5.4 詳細説明

a) 用語
   - C&A –組織の内部要求に従って行われる認証，認定及びセキュリティ評価のこと
     承認権限者[AO]－システムの導入を正式に認証する権限をもつグループ又は個人

b) 計数ルール
   - 報告期間内において導入された新システムの数
   - 報告期間内において導入され，導入の前に運用認可を受けた新システムの数

c) 計数ルールの除外
   組織がシステムインベントリを維持しない，正式な C&A プロセス（CA-1）を導入しない，又は全てのシステムに対し導入前に C&A のプロセスの完了を要求しない場合は，除外は無効となる。

d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
CACM	**C&A 完了測定**	(導入前に AO 認可された C&A パッケージを完了した新システムの数) / (新しく導入されたシステムの全数)	導入前に認定された新システムの比率は組織によって設定された高い数値であることが望ましい

2.5.5 データ発生源

システムインベントリ，システム C&A 文書

2.5.6 報告頻度

組織が定める（例：毎年)

2.5.7 測定法出典

NIST – SP800-53, CA-6

2.6 Configuration Changes Measure

2.6.1 General Description and Title

Configuration Changes Measure measures the percentage of approved and implemented configuration changes identified in the latest automated baseline configuration.

2.6.2 Purpose

Accelerate the development and use of an electronic information infrastructure. Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

2.6.3 Applicable Categories

Core Network Products. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

2.6.4 Detailed Description

a) Terminology

None

b) Counting Rules

- Number of configuration changes identified through automated scanning over the last reporting period
- Number of change control requests approved and implemented over the last reporting period

c) Counting Rule Exclusions

- Invalid exclusions will result for organizations that do not manage configuration changes using a formal and approved process (CM-3) and for organizations that do not use automated tools to identify configuration changes on systems/networks.

d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
CCM	Change Control Measure	(number of approved and implemented configuration changes identified in the latest automated baseline configuration) / (total number of configuration changes identified through automated scans)	% of approved changes to detected changes should be a high number set by the organization

2.6.5 Sources of Data

System security plans, configuration management database, security tools logs

2.6.6 Reporting Frequency

Organization defined (example: annually)

2.6.7 Source of Measurement

NIST – SP800-53, CM-2/CM-3

2.6 構成変更測定

2.6.1 一般

構成変更測定は，最新の自動化したベースライン構成で確認された承認，実施済みの構成変更の比率を測定する。

2.6.2 目的

電子情報インフラの発展と使用を促進する。それぞれのシステム開発ライフサイクルを通して，
組織の情報システム（ハードウェア，ソフトウェア，ファームウェアとドキュメンテーションを含む）のベースライン構成とインベントリを作成・維持する。

2.6.3 適用する製品分類

コアネットワーク製品。製品分類表の最新版は
http://tl9000.org/resources/resources.html を参照。

2.6.4 詳細説明

a) 用語

なし

b) 計数ルール

- 直近の報告期間の自動化スキャンニングで識別された構成変更の数
- 直近の報告期間の承認済み，実施済みの変更管理要求の数

c) 計数ルールの除外

組織が正式な，承認されたプロセス（CM-3）を使用して構成変更管理を実施しない場合，及び組織がシステム/ネットワーク上で構成変更を識別するための自動化ツールを使用しない場合には除外が無効となる。

d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
CCM	構成変更測定 [訳注：原文誤記]	(最新の自動化ベースライン構成で確認された承認，実施済みの構成変更の数)/（自動化スキャンで確認された構成変更の合計数）	検出された変更に対する承認された変更の比率は，組織によって設定された高い数字であることが望ましい

2.6.5 データ発生源

システムセキュリティ計画，構成管理データベース，セキュリティツールログ

2.6.6 報告頻度

組織が定める（例：毎年）

2.6.7 測定法出典

NIST – SP800-53, CM-2/CM-3

2.7 Contingency Plan Testing Measure

2.7.1 General Description and Title

Contingency Plan Testing Measure measures the percentage of information systems that have conducted annual contingency plan testing

2.7.2 Purpose

Ensure an environment of comprehensive security and accountability for personnel facilities and systems. Establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

2.7.3 Applicable Categories

All Product Categories. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

2.7.4 Detailed Description

a) Terminology

None

b) Counting Rules

- Systems in Inventory
- Systems with approved contingency plan
- Contingency plans successfully tested within the year

c) Counting Rule Exclusions

None

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
CPTM	Contingency Plan Testing Measure	Number of information systems that have conducted annual contingency plan testing / Number of information systems in the system inventory	% information systems that have conducted annual plan testing

2.7.5 Sources of Data

Contingency plan testing results.

2.7.6 Reporting Frequency

Organization defined (example annually)

2.7.7 Source of Measurement

NIST – SP800-53, CP-4

2.7 緊急時対応計画試験測定

2.7.1 一般

緊急時対応計画試験測定は，毎年，緊急時対応計画試験が実施される情報システムの比率を測定する。

2.7.2 目的

要員，設備及びシステムに対する包括的なセキュリティ環境及びアカウンタビリティを確実にする。緊急事態における重要な情報リソースの可用性及び業務の継続性を確実にするために，組織の情報システムに対する，緊急時の対応，バックアップ業務，及び災害後の復旧の計画を，確立し，維持し，効果的に実現する。

2.7.3 適用する製品分類

全ての製品分類。 製品分類表の最新版は
http://tl9000.org/resources/resources.html を参照。

2.7.4 詳細説明

a) 用語

なし。

b) 計数ルール

- 保有しているシステム数
- 承認された緊急時対応計画のあるシステム数
- その年に成功裏に試験が実施された緊急時対応計画数

c) 計数ルールの除外

なし

d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
CPTM	緊急時対応計画試験測定	（毎年緊急時対応計画試験を実施している情報システム数）/ （保有している情報システム数）	毎年試験を実施している情報システムの比率

2.7.5 データ発生源

緊急時対応計画の試験結果。

2.7.6 報告頻度

組織が定める（例：毎年）

2.7.7 測定法出典

NIST – SP800-53, CP-4

2.8 User Accounts Measure

2.8.1 General Description and Title

User Accounts Measure measures the percentage of users with access to shared accounts.

2.8.2 Purpose

Ensure an environment of comprehensive security and accountability for personnel, facilities, and products. All system users are identified and authenticated in accordance with information security policy.

2.8.3 Applicable Categories

All Product Categories. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

2.8.4 Detailed Description

a) Terminology
   - Shared account – Any account that is not unique or intended for use by a single user.

b) Counting Rules
   - Number of users with access to the system
   - Number of users with access to shared accounts

c) Counting Rule Exclusions
   None

d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
UAM	User Accounts Measure	(number of users with access to shared accounts) / (total number of users)	% of users with access to shared accounts (should be a low number set by the organization)

2.8.5 Sources of Data

Configuration management database, access control list, system-produced user ID list

2.8.6 Reporting Frequency

Organization defined (example: monthly)

2.8.7 Source of Measurement

NIST – SP800-53, AC-2/AC-3/IA-2

2.8 ユーザアカウント測定

2.8.1 一般

ユーザアカウント測定は，共有されるアカウントへアクセスするユーザの比率を測定する。

2.8.2 目的

要員，設備及び製品に対する包括的なセキュリティ環境及びアカウンタビリティを確実にする。すべてのシステムユーザは，情報セキュリティ方針に従って，特定され，認証される。

2.8.3 適用する製品分類

全ての製品分類。製品分類表の最新版は
http://tl9000.org/resources/resources.html を参照。

2.8.4 詳細説明

a) 用語
   - 共有アカウントーユニークではない，又は単一のユーザによる使用を意図していないアカウント。

b) 計数ルール
   - システムへアクセスするユーザ数
   - 共有アカウントにアクセスするユーザ数

c) 計数ルールの除外
   なし

d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
UAM	ユーザアカウント測定	（共有アカウントへアクセスするユーザ数）/ （全ユーザ数）	共有アカウントへアクセスするユーザの比率（組織によって設定された低い数値であることが望ましい）

2.7.8 データ発生源

構成管理データベース，アクセス制御リスト，システムが生成したユーザ ID リスト。

2.7.9 報告頻度

組織が定める（例：毎月）

2.7.10 測定法出典

NIST – SP800-53, AC-2/AC-3/IA-2

2.9 Incident Response Measure

2.9.1 General Description and Title

Incident Response Measure measures the percentage of incidents reported within required time frame per applicable incident category (the measure should be computed for each incident category).

2.9.2 Purpose

Make accurate, timely information on the organization's programs and services readily available. Track, document, and report incidents to appropriate organizational officials and/or authorities.

2.9.3 Applicable Categories

Core Network Products and End Customer Services. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

2.9.4 Detailed Description

a) Terminology

None

b) Counting Rules

- Number of incidents reported during the reporting period for the following categories: unauthorized access, denial of service, malicious code, improper usage, scans/probes/attempted access, and investigation
- Number of incidents reported within the prescribed time frame established by US-CERT for each category

c) Counting Rule Exclusions

None

d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
IRM	Incident Response Measure	For each category: (number of incidents reported on time) / (total number of incidents reported for that category)	% of incidents reported in an appropriate timeframe should be a high number set by the organization

2.9.5 Sources of Data

Incident logs, incident tracking database

2.9.6 Reporting Frequency

Organization defined (example: annually)

2.9.7 Source of Measurement

NIST – SP800-53, IR-6

2.9 インシデント対応測定

2.9.1 一般

インシデント対応測定は，適用するインシデント分類ごとに要求された期間内に報告されたインシデントの比率を測定する (測定はインシデント分類ごとに計算されることが望ましい)

2.9.2 目的

組織のプログラムとサービスに関する正確でタイムリーな情報を容易に使用できるようにする。
インシデントを，追跡し，文書化し，組織の適切な責任者及び/又は関係当局に報告する。

2.9.3 適用する製品分類

コアネットワーク製品及びエンドユーザサービス。製品分類表の最新版は
http://tl9000.org/resources/resources.html を参照。

2.9.4 詳細説明

a) 用語

なし

b) 計数ルール

- 以下の分類につき，報告期間内で報告されたインシデントの数：
  不正アクセス，サービス妨害，悪意のコード，不適切な使用，スキャン/プローブ/アクセス試行及び調査
- 分類ごとに US-CERT が定めた規定期間内に報告されたインシデントの数。

c) 計数ルールの除外

なし

d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
IRM	インシデント対応測定	分類ごと: (時間通りに報告されたインシデントの数) / (該当する分類で報告された全てのインシデントの数)	妥当な期間内における報告されたインシデントの比率は，組織によって設定された高い数値であることが望ましい

2.9.5 データ発生源

インシデントログ，インシデント追跡データベース

2.9.6 報告頻度

組織が定める （例: 毎年)

2.9.7 測定法出典

NIST – SP800-53, IR-6

2.10 Media Sanitization Measure

2.10.1 General Description and Title

Media Sanitization Measure measures the percentage of media that passes sanitization testing.

2.10.2 Purpose

Ensure an environment of comprehensive security and accountability for personnel, facilities, and products. Sanitize or destroy information system media before disposal or release for reuse.

2.10.3 Applicable Categories

Core Network Products. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

2.10.4 Detailed Description

a) Terminology

None

b) Counting Rules

- Number of media that successfully passed sanitization testing
- Total number of media tested

c) Counting Rule Exclusions

- Invalid exclusions will result for organizations that do not set policy requirements for media sanitization (MP-1) or define media sanitization procedures (e.g. FIPS-199, high impact systems [MP-6, Enhancement 2]).

d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
MSM	Media Sanitization Measure	(number of media that pass sanitization procedures testing) / (total number of media tested)	% of media successfully sanitized according to established procedures should be a high number set by the organization

2.10.5 Sources of Data

Sanitization testing results

2.10.6 Reporting Frequency

Organization defined (example: annually)

2.10.7 Source of Measurement

NIST – SP800-53, MP-6

2.10 媒体上の記録抹消測定

2.10.1 一般

媒体上の記録抹消測定は，媒体上の記録抹消試験に合格した媒体の比率を測定する。

2.10.2 目的

要員，設備及び製品に対する包括的なセキュリティ環境及びアカウンタビリティを確実にする。情報システムの媒体を廃棄又は再利用のために手放す前に，媒体上の記録を抹消する，又は媒体を破壊する。

2.10.3 適用する製品分類

コアネットワーク製品。 製品分類表の最新版は

http://tl9000.org/resources/resources.html.を参照。

2.10.4 詳細説明

a) 用語

なし

b) 計数ルール

- 成功裏に媒体上の記録抹消試験に合格した媒体の数
- 試験した媒体の総数

c) 計数ルールの除外

組織が，媒体上の記録抹消の方針要求事項（MP-1）を設定していない，又は媒体上の記録抹消手順（例えば FIPS-199 high impact systems [MP-6, Enhancement 2]を規定していない場合は，除外は無効 となる。

d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
MSM	媒体上の記録抹消測定	(成功裏に媒体上の記録抹消試験を合格した媒体の数) / (試験した媒体の総数)	確立された手順により成功裏に媒体上の記録抹消された媒体の比率は 組織によって設定された高い数値であることが望ましい。

2.10.5 データ発生源

媒体上の記録抹消試験結果

2.10.6 報告頻度

組織が定める（例：毎年)

2.10.7 測定法出典

NIST – SP800-53, MP-6

2.11 Physical Security Incidents Measure

2.11.1 General Description and Title

Physical Security Incidents Measure measures the percentage of physical security incidents allowing unauthorized entry into facilities containing information systems.

2.11.2 Purpose

Ensure an environment of comprehensive security and accountability for personnel, facilities, and products. Integrate physical and information security protection mechanisms to ensure appropriate protection of the organization's information resources.

2.11.3 Applicable Categories

All Product Categories. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

2.11.4 Detailed Description

a) Terminology

None

b) Counting Rules

- Number of physical security incidents occurring during the specified period
- Number of physical security incidents resulting in unauthorized entry into facilities containing information systems

c) Counting Rule Exclusions

None

d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
PSIM	Physical Security Incidents Measure	(number of physical security incidents allowing entry into facilities containing information systems) / (total number of physical security incidents)	% of physical security incidents resulting in unauthorized access should be a low number set by the organization

2.11.5 Sources of Data

Physical security incident reports, physical access control logs

2.11.6 Reporting Frequency

Organization defined (example: quarterly)

2.11.7 Source of Measurement

NIST – SP800-53, PE-6

2.11 物理的セキュリティインシデント測定

2.11.1 一般

物理的セキュリティインシデント測定は，情報システムを含む設備への無許可の侵入を許す物理的セキュリティインシデントの比率を測定する。

2.11.2 目的

要員，設備及び製品に対する包括的なセキュリティ環境及びアカウンタビリティを確実にする。物理的セキュリティ保護と情報セキュリティ保護の仕組みを統合して，組織の情報リソースの適切な保護を確実にする。

2.11.3 適用する製品分類

全ての製品分類。製品分類表の最新版は，

http://tl9000.org/resources/resources.html を参照

2.11.4 詳細説明

a) 用語

なし

b) 計数ルール

- 定められた期間中に発生する物理的セキュリティインシデント数
- 情報システムを含む設備への無許可の侵入となる物理的セキュリティインシデント数

c) 計数ルールの除外

なし

d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
PSIM	物理的セキュリティインシデント測定	(情報システムを含む設備への無許可の侵入を許す物理的セキュリティインシデント数) / (物理的セキュリティインシデントの総数) [訳注：原文 unauthorized 抜け]	無許可のアクセスとなる物理的セキュリティインシデントの比率は，組織によって設定された低い数値であることが望ましい。

2.11.5 データ発生源

物理的セキュリティインシデント報告，物理的アクセス管理記録

2.11.6 報告頻度

組織が定める（例：四半期毎）

2.11.7 測定法出典

NIST – SP800-53, PE-6

2.12 Planning Measure

2.12.1 General Description and Title

Planning Measure measures the percentage of employees who are authorized access to information systems only after they sign an acknowledgement that they have read and understood rules of behavior.

2.12.2 Purpose

Ensure an environment of comprehensive and accountability for personnel, facilities, and products. Develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for information systems, and the rules of behavior for individuals accessing these systems.

2.12.3 Applicable Categories

All Product Categories. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

2.12.4 Detailed Description

a) Terminology

None

b) Counting Rules

- Number of users that are granted access after signing rules of behavior acknowledgement
- Number of users that access the system

c) Counting Rule Exclusions

- Invalid exclusions will result if no formal rules of behavior policies exist (PL-4)

d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
PM	Planning Measure	(number of users who are granted system access after signing a rules of behavior acknowledgement) / (total number of users with system access)	% of users accessing the system and having signed the rules of behavior should be a high number set by the organization

2.12.5 Sources of Data

Rules of behavior acknowledgment records

2.12.6 Reporting Frequency

Organization defined (example: annually)

2.12.7 Source of Measurement

NIST – SP800-53, PL-4/AC-2

2.12 計画作成測定

2.12.1 一般

計画作成測定は，行動規則を読み，理解したことの同意書に署名した後にのみ情報システムにアクセスする権限を与えられた従業員の比率を測定する。

2.12.2 目的

要員，設備及び製品に対する包括的なセキュリティ環境及びアカウンタビリティを確実にする。実施中又は計画中の，組織の情報システムに対するセキュリティ管理策及びこれらのシステムへの個人のアクセスに対する行動規則を記述した，組織の情報システムに対するセキュリティ計画を，開発し，文書化し，定期的に更新し，導入する。

2.12.3 適用する製品分類

全ての製品分類。製品分類表の最新版は
http://tl9000.org/resources/resources.html を参照。

2.12.4 詳細説明

a) 用語

なし

b) 計数ルール

- 行動規則の同意書に署名をした後にアクセスを許可されたユーザの数
- システムにアクセスするユーザの数

c) 計数ルールの除外

- 正式な行動規則方針がない場合，除外は無効となる（PL-4）

d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
PM	計画作成測定	(行動規則の同意書に署名をした後にアクセスを許可されたユーザの数) / (システムにアクセスするユーザの総数)	システムにアクセスしているユーザで行動規則に署名している比率は組織によって設定された高い数値であることが望ましい。

2.12.5 データ発生源

行動規則同意書の記録

2.12.6 報告頻度

組織が定める（例：毎年）

2.12.7 測定法出典

NIST – SP800-53, PL-4/AC-2

2.13 Personnel Security Measure

2.13.1 General Description and Title

Personnel Security Measure measures the percentage of individuals screened prior to being granted access to organizational information and information systems.

2.13.2 Purpose

Ensure an environment of comprehensive and accountability for personnel, facilities, and products. Ensure that individuals occupying positions of responsibility within organizations are trustworthy and meet established security criteria for those positions.

2.13.3 Applicable Categories

All Product Categories. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

2.13.4 Detailed Description

a) Terminology

None

b) Counting Rules

- Number of individuals granted access to organizational information and information systems
- Number of individuals that have completed personnel screening

c) Counting Rule Exclusions

None

d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
PSM	Personnel Security Measure	(number of individuals screened) / (total number of individuals with access)	% of users screened prior to being granted system access should be a high number set by the organization

2.13.5 Sources of Data

Clearance records, access control lists

2.13.6 Reporting Frequency

Organization defined (example: annually)

2.13.7 Source of Measurement

NIST – SP800-53, PS-3/AC-2

2.13 要員セキュリティ測定

2.13.1 一般

要員セキュリティ測定は，組織の情報及び情報システムへのアクセスを許可される前に，審査される個人の比率を測定する。

2.13.2 目的

要員，設備及び製品に対する包括的なセキュリティ環境及びアカウンタビリティを確実にする。組織内の責任ある地位にある個人が信頼でき，それら地位についての確立されたセキュリティ基準に適合することを確実にする。

2.13.3 適用する製品分類

全ての製品分類。製品分類表の最新版は http://tl9000.org/resources/resources.html を参照。

2.13.4 詳細説明

a) 用語

なし

b) 計数ルール

- 組織の情報及び情報システムへのアクセスを許可されている人数
- 要員適性審査を完了した人数

c) 計数ルールの除外

なし

d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
PSM	要員セキュリティ測定	（適性審査された人数）/（アクセスする総数）	システムへのアクセスを許可される前に審査されるユーザの比率は組織によって設定された高い数値であることが望ましい。

2.13.5 データ発生源

審査通過記録，アクセス制御リスト

2.13.6 報告頻度

組織が定める（例：毎年）

2.13.7 測定法出典

NIST – SP800-53, PS-3/AC-2

2.14 Risk Assessment Vulnerability Measure

2.14.1 General Description and Title

Risk Assessment Vulnerability Measure measures the percentage of vulnerabilities remediated within organization-specified time frames.

2.14.2 Purpose

Ensure an environment of comprehensive accountability for personnel, facilities, and products. Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals resulting from the operation of organizational information systems.

2.14.3 Applicable Categories

All Product Categories. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

2.14.4 Detailed Description

a) Terminology
   - POA&M – Plan of Actions and Milestones

b) Counting Rules
   - Number of vulnerabilities identified through vulnerability scanning
   - Number of vulnerabilities remediated on schedule according to the POA&M

c) Counting Rule Exclusions
   - Invalid exclusions will result if a periodic scans do not occur in a timely manner (RA-5) or if no formal processes are defined for the documentation and remediation of vulnerabilities identified (e.g. – POA&M, [CA-5])

d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
RAVM	Risk Assessment Vulnerability Measure	(number of vulnerabilities remediated in accordance with POA&M schedule) / (total number of POA&M-documented vulnerabilities identified through vulnerability scans)	% of vulnerabilities remediated in accordance with established timelines should be a high number set by the organization

2.14.5 Sources of Data

POA&Ms, vulnerability scanning reports

2.14.6 Reporting Frequency

Organization defined (example: monthly)

2.14.7 Source of Measurement

NIST – SP800-53, RA-5/CA-5

2.14 脆弱性リスクアセスメント測定

2.14.1 一般

脆弱性リスクアセスメント測定は，組織が規定した期限内に修正された脆弱性の比率を測定する。

2.14.2 目的

要員，設備及び製品に対する包括的なセキュリティ環境及びアカウンタビリティを確実にする。組織の情報システム運営に起因する，組織運営（使命，機能，イメージ，又は評判を含む），組織資産，及び個人に対するリスクを定期的に評価する。

2.14.3 適用する製品分類

全ての製品分類。製品分類表の最新版は
http://tl9000.org/resources.html.を参照。

2.14.4 詳細説明

a) 用語
   ・POA&M –活動計画とマイルストーン

b) 計数ルール
   ・脆弱性スキャンを通して識別された脆弱性の数
   ・POA&M に従って，スケジュール通りに修正された脆弱性の数

c) 計数ルールの除外
・定期的なスキャンが適時の方法で実施されない場合（RA-5），又は特定された脆弱性の文書化及び修正に対する正式なプロセスが規定されていない場合（例：POA&M，[CA - 5]），除外は無効となる。

d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
RAVM	脆弱性リスクアセスメント測定	（POA&M スケジュールに従って修正された脆弱性の数）／(POA&M の総数 - 脆弱性スキャンを通して識別され文書化された脆弱性の数)	設定された予定表に従って修正された脆弱性の比率は，組織によって設定された高い数値であることが望ましい。

2.14.5 データ発生源

POA&Ms，脆弱性のスキャン報告

2.14.6 報告頻度

組織が定める（例：毎月）

2.14.7 測定法出典

NIST - SP800-53, RA - 5/CA - 5

2.15 Service Acquisition Contract Measure

2.15.1 General Description and Title

Service Acquisition Contract Measure measures the percentage of system and service acquisition contracts that include security requirements and/or specifications.

2.15.2 Purpose

Accelerate the development and use of an electronic information infrastructure. Ensure third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

2.15.3 Applicable Categories

All Product Categories. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

2.15.4 Detailed Description

a) Terminology

None

b) Counting Rules

- Number of active service acquisition contracts the organization has
- Number of active service acquisition contracts that include security requirements and specifications

c) Counting Rule Exclusions

None

d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
SACM	Service Acquisition Contract Measure	(number of system and service acquisition contracts that include security requirements) / (total number of system and service acquisition contracts)	% of contracts that contain security requirements should be a high number set by the organization

2.15.5 Sources of Data

System and service acquisition contracts

2.15.6 Reporting Frequency

Organization defined (example: annually)

2.15.7 Source of Measurement

NIST – SP800-53, SA-4

2.15 サービス調達契約測定

2.15.1 一般

サービス調達契約測定は，セキュリティ要件及び/又は仕様を含むシステム及びサービス調達契約の比率を測定する。

2.15.2 目的

電子情報インフラの開発と使用を促進する。 第三者プロバイダが，組織からの外部委託により提供する情報，アプリケーション及び/又はサービスを保護するために適切なセキュリティ対策を採用することを確実にする。

2.15.3 適用する製品分類

全ての製品分類。製品分類表の最新版は
http://tl9000.org/resources/resources.html を参照。

2.15.4 詳細説明

a)用語

なし

b) 計算ルール

- 組織保有の有効サービス調達契約数。
- セキュリティ要件と仕様を含む有効サービス調達契約数

c)計数ルールの除外

なし

d)計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
SACM	サービス調達契約測定	(セキュリティ要件を含むシステム及びサービス調達契約数)/ (システム及びサービス調達契約総数)	セキュリティ要件を含む契約の比率は，組織によって設定された高い数値であることが望ましい。

2.15.5 データの発生源

システム及びサービス調達契約

2.15.6 報告頻度

組織が定める（例: 毎年)

2.15.7 測定法出典

NIST - SP800-53, SA-4

2.16 System and Communication Protection Measure

2.16.1 General Description and Title

System and Communication Protection Measure measures the percentage of mobile computers and devices that perform all cryptographic operations using validated cryptographic modules operating in approved modes.

2.16.2 Purpose

Accelerate the development and use of an electronic information infrastructure. Allocate sufficient resources to adequately protect electronic information infrastructure.

2.16.3 Applicable Categories

All Product Categories. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

2.16.4 Detailed Description

a) Terminology

None

b) Counting Rules

- Number of mobile computers and devices used in the organization
- Number of mobile computers that employ cryptography
  - Number of mobile computers and devices using validated encryption methods
  - Number of mobile computers and devices using approved encryption modules

c) Counting Rule Exclusions

- Invalid exclusions will result if no standardized and formal encryption methods/modes are identified for organizational use (e.g. – FIPS 140-2)

d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
SCPM	System and Communication Protection Measure	(number of mobile computers and devices using validated cryptographic modules and methods) / (total number of mobile computers and devices)	% of mobile computers and devices using approved cryptographic modes and methods should be a high number set by the organization

2.16.5 Sources of Data

System security plans

2.16.6 Reporting Frequency

Organization defined (example: annually)

2.16.7 Source of Measurement

NIST – SP800-53, SC-13

2.16 システム及び通信保護測定

2.16.1 一般

システム及び通信保護測定は，承認されたモードで動作する，有効性が確認されている暗号モジュールを用いて，全て暗号運用するモバイルコンピュータ及び携帯機器の比率を測定する。

2.16.2 目的

電子情報インフラの開発と使用を促進する。 適切に電子情報インフラを保護するための十分な資源を割り当てる。

2.16.3 適用する製品分類

全ての製品分類。 製品分類表の最新版は
http://tl9000.org/resources/resources.html を 参照。

2.16.4 詳細説明

a) 用語

なし

b) 計数ルール

- 組織内のモバイルコンピュータ及び携帯機器の数
- 暗号実装のモバイルコンピュータ及び携帯機器の数
  - 有効性が確認された暗号方式を使用するモバイルコンピュータ及び携帯機器の数
  - 承認された暗号モジュールを使用するモバイルコンピュータ及び携帯機器の数

c) 計数ルールの除外

組織で使用する標準化された正式な暗号方式/モードが特定されていない場合 (例： FIPS 140-2)，除外は無効となる。

d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
SCPM	システム及び通信保護測定	（有効性が確認された暗号モジュール及び暗号方式を用いるモバイルコンピュータ及び携帯機器の数) /(モバイルコンピュータと携帯機器の総数)	承認された暗号モードと暗号方式を使用するモバイルコンピュータ及び携帯機器の比率は，組織によって設定された高い数値であることが望ましい。

2.16.5 データ発生源

システムセキュリティ計画

2.16.6 報告頻度

組織が定める （例：毎年)

2.16.7 測定法出典

NIST – SP800-53, SC-13

2.17 Flaw Remediation Measure

2.17.1 General Description and Title

Flaw Remediation measures the percentage of operating system vulnerabilities for which patches have been applied or that have otherwise been mitigated.

2.17.2 Purpose

Accelerate the development and use of an electronic information infrastructure. Provide protection from malicious code at appropriate locations within organizational information systems, monitor information systems security alerts and advisories, and take appropriate actions in response.

2.17.3 Applicable Categories

All Product Categories. For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

2.17.4 Detailed Description

a) Terminology
   - POA&M – Plan of Actions and Milestones

b) Counting Rules
   - Number of vulnerabilities identified by analyzing distributed alerts and advisories
   - Number of alerts identified through vulnerability scans
   - Number of patches or work-arounds implemented to address identified vulnerabilities
   - Number of vulnerabilities determined to be non-applicable
   - Number of waivers granted for weaknesses that could not be identified by implementing patches or work-arounds

c) Counting Rule Exclusions

None

d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
FRM	Flaw Remediation Measure	(number of vulnerabilities addressed in alerts for which patches were implemented, non-applicable, or waived) / (total number of applicable vulnerabilities identified through alerts and scans)	% of total vulnerabilities addressed should be a high number set by the organization

2.17.5 Sources of Data

System security plans

2.17.6 Reporting Frequency

Organization defined (example: monthly)

2.17.7 Source of Measurement

NIST – SP800-53, SI-2

2.17 欠陥修正測定

2.17.1 一般

欠陥修正測定は，パッチを適用したり別の方法で軽減されたオペレーティングシステムの脆弱性の比率を測定する。

2.17.2 目的

電子情報インフラの開発と利用を促進する。また，組織の情報システムの中の適切な場所において悪意のコードから保護し，情報システムセキュリティ警報及び勧告を監視し，適切な対応活動を実施する。

2.17.3 適用する製品分類

全ての製品分類。製品分類表の最新版は

http://tl9000.org/resources/resources.html を参照。

2.17.4 詳細説明

a) 用語
   - POA&M –活動計画とマイルストーン

b) 計数ルール
   - 配信された警報やアドバイザリーを分析することで識別された脆弱性の数
   - 脆弱性のスキャンにより識別された警報の数
   - 識別された脆弱性を処置するためのパッチ，又は回避策の数
   - 非適用と決めた脆弱性の数
   - パッチ，又はは回避策の実施では対処できない弱点に対して許可された対処放棄の数

c) 計数ルールの除外

なし

d) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
FRM	欠陥修正測定	警報で対処された脆弱性で，パッチが導入された，不適用となった，又は対処放棄された数 / 警報やスキャンにより識別された適用可能な脆弱性の総数	対処された脆弱性の比率は，組織によって設定された高い数値であることが望ましい。

2.17.5 データ発生源

システムセキュリティ計画

2.17.6 報告頻度

組織が定める（例：毎月）

2.17.7 測定法出典

NIST – SP800-53, SI-2

3.1 Security Related Outages

3.1.1 General Description and Title

Basically the outages included in SRO are a subset of those in SONE (see Section 6.2 of TL 9000 Measurement Handbook) but the outages may be counted, tracked, and reported separately in order to focus on addressing security defects.

3.1.2 Purpose

The SRO measurement can provide insight into the impact of network element (NE) security vulnerabilities in the field, or can indicate gaps in wider security controls in the environment into which the element is deployed (for example, de-facto controls against denial-of-service attacks or malware). As such, the SRO measurement can provide data to help evaluate the efficacy of NE capabilities against attacks that the NE security vulnerabilities during product operation, and to help evaluate the efficacy of security controls and security operations in the deployment environment.

3.1.3 Applicable Categories

Product categories 1~6 in Table A-2, TL 9000 Measurement Applicability Table (Normalized Units). For the latest version of the Product Category Table see http://tl9000.org/resources/resources.html.

3.1.4 Detailed Description

The criteria for distinguishing between customer- and product-attributable outages as described in the following counting rules are very high-level and indicative and, as such, would require interpretation for every separate usage.

The applicability and usefulness of this metric across a range of network element types requires investigation and elaboration. For example, the security requirements for a layer 2 switch are very different to those for an application server. Also, for example, one hour outage on a core switch (of which there are few in the network) is very much more serious than one hour outage of an access device (of which there may be a vast number deployed). While maintaining the four metrics for each network element type would be unwieldy, aggregating and counting the outages for a range of network elements into one result may not be appropriate.

a) Terminology
   Outage
b) Counting Rules:
   - Outages for submission under All Causes include Customer Attributable Outage and Product Attributable Outage;
   - Counting rules 3, 4, 5, 6, and 7 in Section 6.1.4 b) of the TL 9000 Measurement Handbook shall be applied;
   - All outages caused by a security issue that result in a complete loss of primary functionality for all or part of the system for duration greater than 15 seconds during the operational window (see Table A-3 Network Element Impact Outage Definitions in TL 9000 Measurement Handbook). Security issues include:
     - Virus, worms
     - Hackers attacks based on product defects
     - Denial of Services attacks based on product defects
     - Other attacks based on product defects.
   - Only outages directly caused by a security incident are counted. Outages due to an operational decision to take an element or system offline to protect against attack are not included.
   - A product attributable outage can be caused by any of the following security reasons:
     - Security intrusion exploiting product vulnerabilities against which the product was required to be hardened;
     - Denial of Services attacks exploiting product vulnerabilities against which the product was required to be resilient;

3.1 セキュリティ関連 停止 (SRO)

3.1.1 一般

基本的に SRO に含まれている停止は，SONE(TL 9000 測定法ハンドブック 6.2 章参照)の停止の一部であるが，セキュリティ欠陥に注目するために，停止は別々に計数，追跡，及び報告してもよい。

3.1.2 目的

SRO 測定法はフィールドにおけるネットワークエレメント(NE)のセキュリティ脆弱性の影響を把握でき，又は，そのネットワークエレメント設置環境でのより広範なセキュリティ管理策におけるギャップを示すものである。(例えば，サービス妨害攻撃又は悪意あるソフトに対するデファクト管理策)
このように，SRO 測定法は，製品運用中の NE のセキュリティ脆弱性を悪用する攻撃に対する NE 能力の有効性の評価を助けるデータを提供する。そして，設置環境でのセキュリティ管理策とセキュリティオペレーションの有効性の評価を支援する。

3.1.3 適用する製品分類

TL9000 測定法適用表(規準化単位)の表 A-2 の製品分類 1~6。
製品分類表の最新版は
http://tl9000.org/resources/resouces.html を参照。

3.1.4 詳細説明

以下の計数ルールで示す顧客起因と製品起因停止の識別基準は高度かつ暗示的であるため，全ての別々の用法に対する解釈が必要となる。
ネットワークエレメントタイプの全範囲に亘って，この測定法の適用と利用は入念な調査と精緻化を要する。例えば，レイヤ２スイッチへのセキュリティ要求はアプリケーションサーバへの要求とは大きく異なる。また，例えば，コアスイッチ（ネットワーク内に殆どないが）の１時間停止は，アクセスデバイス（ネットワーク内に厖大な数が配置されている）の１時間停止よりもはるかに重大である。
各ネットワークエレメントタイプに対し 4 つの測定法を維持することは容易ではないが，広範なネットワークエレメントの停止を一つの結果として集め計数することは適切ではないだろう。

a) 用語
   停止
b) 計数ルール
   - 全ての原因に基づき提出する停止には顧客起因停止及び製品起因停止を含む；
   - TL9000 測定法ハンドブック，セクション６．１．４ｂ）の計数ルール３，４，５，６，及び７を適用しなければならない；
   - 運用期間において 15 秒間を超えるシステムのすべて，又は一部の基本的な機能の完全な損失となる，運用時間帯の１５秒以上に亘る，全システム又は部分システムに対して主要な機能の完全喪失を引き起こすことになる，セキュリティ問題によるすべての停止。そのセキュリティ問題には次を含む；
     - ウイルス，ワーム
     - 製品欠陥に基づくハッカー攻撃
     - 製品欠陥に基づくサービス妨害攻撃
     - 製品欠陥に基づくその他の攻撃
   - セキュリティインシデントが直接原因の停止（動作不能）のみを計数する。運用上の判断により，攻撃防御のためにエレメントやシステムを切り離すことによる停止は含めない。
   - 製品起因(product attribute)の停止（動作不能）は次のセキュリティ理由による：
     - 要求されている耐力の脆弱性を悪用されたセキュリティ侵入
     - 要求されている回復力の脆弱性を悪用されたサービス妨害攻撃

- A customer attributable outage can be caused by any of the following security reasons:
  - Vulnerabilities due to miss-configuration or due to not following any supplier instructions and guidelines on secure deployment and use of the product
  - Attacks exploiting any weakness of a customer organization's internal policy that fails to follow the best practice for network security (e.g. bad security configurations, deploying no firewalls or anti-DOS devices etc.)
  - Customer's internal security management enforcement issues (e.g. users with access to shared accounts, password leakage etc.)
  - Associated security patches are not deployed by the customer;
  - Associated anti-virus solution or virus library is not updated by the customer;

c) Counting Rule Exclusions:

- Counting rule exclusions 2, 3, 4, 5, 6 and 7 in Section 6.1.4 c) of the Measurement Handbook shall be applied;
- If, as a matter of internal policy, a SP organization fails to follow the best practice for network security (e.g. not deploying anti-virus solution, firewalls or anti-DOS devices etc.), then the resultant outages shall be attributed to SRO1 and SRO2;
- Outages due to customer's internal management problems (users with access to shared accounts, etc.) shall be attributed to SRO1 and SRO2.

d) Calculations and Formulas

Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
SRO1	Security related customer attributable outage frequency	(number of customer caused outages) / (number of NEs in service)	customer caused outages per NE
SRO2	Security related customer attributable outage downtime	(sum of durations of customer caused outage) / (number of NEs in service)	minutes of customer caused outages per NE
SRO3	Security related product attributable outage frequency	(number of product caused outages) / (number of NEs in service)	product caused outages per NE
SRO4	Security related product attributable outage downtime	(sum of durations of product caused outage) / (number of NEs in service)	minutes of product caused outages per NE

3.1.5 Sources of Data

Information provided by customers

3.1.6 Reporting Frequency

Monthly is recommended but can be reported quarterly or annually.

3.1.7 Source of Measurement

QuEST Forum NGN Security Sub Team

- 顧客起因(customer attribute)の停止（動作不能）は次のセキュリティ理由による：
  - 間違った構成，又は，製品の使い方や安全な設置を供給者説明書やガイドライン通りにしなかった為の脆弱性。
  - ネットワークセキュリティのベストプラクティスに従わない顧客内部のポリシーの弱さを攻撃（例えば，ファイアウォール又は Anti-DOS デバイスが設置されていないなど，脆弱なセキュリティ構成）顧客内部セキュリティ管理の問題　（例えば，アカウントの共有，パスワードの漏洩）
  - 顧客がセキュリティパッチしなかった問題
  - 顧客がウィルス対策やウィルスライブラリを更新しなかった問題

c) 計数ルールの除外

- 測定法ハンドブックのセクション 6.1.4 c)の計数のルール除外 2,3,4,5,6 及び 7 に従わなければならない。
- 内部ポリシーの問題で，組織がネットワークセキュリティのベストプラクティスに従わない場合（例えば，ウィルス対策，ファイアウォール，又は Anti-DOS デバイスが設置されていないなど），それによって生ずる停止は SRO1 と SRO2 としなければならない。
- 顧客の内部管理問題（例えば，共有アカウントへ複数のユーザがアクセスするなど）が原因の停止は SRO1 と SRO2 としなければならない。

e) 計算式

測定法識別子及び計算式

識別子	名称	計算式	注記
SRO1	セキュリティ関連顧客起因停止頻度	（顧客起因停止回数）/ (サービス中の NE 数)	NE 一台当たりの顧客起因停止数
SRO2	セキュリティ関連顧客起因停止ダウンタイム	（顧客起因停止時間の合計）/(サービス中の NE 数)	NE 一台当たり顧客起因停止時間（分）
SRO3	セキュリティ関連製品起因停止頻度	（製品起因停止回数）/ (サービス中の NE 数)	NE 一台当たりの製品起因停止数
SRO4	セキュリティ関連製品起因停止ダウンタイム	（製品起因停止時間の合計）/(サービス中の NE 数)	NE 一台当たりの製品起因停止時間（分）

3.1.5 データ発生源

顧客から提供される情報

3.1.6 報告頻度

月次を推奨するが，四半期又は年次報告でもよい

3.1.7 測定法出典

QuEST Forum NGN Security Sub Team
クエストフォーラム NGN セキュリティサブチーム

Glossary

Audit Record
Any log or record related to security such as a security log for a product or access log (physical building or product).

OS Hardening

Out of the box, nearly all operating systems are configured insecurely. The idea of OS hardening is to minimize a computer's exposure to current and future threats by fully configuring the operating system and removing unnecessary applications.

Risk Assessment

The term risk assessment is defined as a process for analyzing a system and identifying the risks from potential threats and vulnerabilities to the information assets or capabilities of the system. Although many methodologies can be used, it should consider threats to the target systems, potential vulnerabilities of the systems, and impact of system exploitation. It may or may not include risk mitigation strategies and countermeasures. Methodologies could include FAIR, OCTAVE or others.

Security Incident

A security incident results in the actual outcomes of a business process deviating from the expected outcomes for confidentiality, integrity & availability due to deficiencies or failures of people, process or technology.

Security Patch

A patch is a modification to existing software in order to improve functionality, fix bugs, or address security vulnerabilities. Security patches are patches that are solely or in part created and released to address one or more security flaws, such as, but not limited to publicly disclosed vulnerabilities.

Vulnerability

Vulnerability is defined as a weakness that could be exploited by an attacker to gain access or take actions beyond those expected or intended

用語解説

監査記録
製品又はアクセスログ（建築物又は製品）へのセキュリティログのような，セキュリティに関するログ又は記録である。

OS 強化
考え方によっては，ほとんどのオペレーティングシステムは不安定に構成されている。 OS 強化の概念は，現在と将来の脅威に対するコンピュータの露出を，オペレーティングシステムを完全に構成し，不要なアプリケーションを取り除くことで最小にすることである。

リスクアセスメント
リスクアセスメント―リスクアセスメントとは，システムを分析し，潜在的脅威及び脆弱性が情報資産又はシステムの機能に与えるリスクを特定するプロセスであると定義される。多くの手法を使用できるが，ターゲットシステムへの脅威，潜在的なシステムの脆弱性，及びシステム悪用の影響を考慮することが望ましい。リスク軽減（低減）のための戦略及び対応を含んでいなくてもよい。 方法論は FAIR(訳注：Factor Analysis of Information Risk)，OCTAVE(訳注：Operationally Critical Thread, Asset and Vulnerability Evaluation)又は他のものを含めることができる。

セキュリティインシデント
セキュリティインシデントは，人，プロセス，技術の欠陥又は不具合により，機密性，完全性及び可用性における，期待される結果に対し，実際のビジネスプロセスの結果に相違をもたらす。

セキュリティーパッチ
パッチは，機能向上，バグ修正，又はセキュリティ脆弱性への対処のために既存のソフトウェアを変更するものである。セキュリティパッチは，単独のパッチとして，又はパッチの一部として作成，リリースされ，１つ又は複数のセキュリティの欠陥，例えば，公開された脆弱性（これに限られるわけではない），に対処するものである。

脆弱性
脆弱性とは，攻撃者による予期又は意図しないアクセス又は行動によって悪用される可能性のある弱点と定義される。