日本ネットワークセキュリティ協会
Japan Network Security Association

JNSA

セキュリティ検査サービス
総合セキュリティ評価基準
（ドラフト　1）

JNSA技術部会
セキュリティ評価WG

JNSA技術部会　セキュリティ評価WG

活動目的

セキュリティ検査結果として、総合セキュリティ評価（いわゆる AA、A+等）を出していますが、お客様から見れば所詮一企業が出しているにすぎず、業界標準といえるものではないと思います。 JNSA参加各社の方々も、独自の評価方法をお持ちと思いますが、今後 BtoBビジネスの発展など、個々の企業のセキュリティレベルのある種の明朗性が重要になると想定され、 JNSAに於いて、中立な立場で、業界標準のセキュリティ評価基準の 実現性と応用範囲（制定時の波及効果）の可能性を探る事を目的とします。

http://www.jnsa.org/index_jnsa_wg.html#technical-dept より

総合セキュリティ評価基準？

JNSA

基準制定のねらい

- **総合評価の明朗性の確保**
  - **総合評価の基準を明確にし、エンドユーザからの信頼を得る**
- **各社が実施している「セキュリティ検査サービス」の結果について、相互評価ができるように標準化する。**
  - **Z社を検査した、A社とB社の結果の比較ができない**
  - **A社によるZ社の評価と、B社によるY社の評価が、比較できない**
- **セキュリティ検査サービスの結果について、把握しやすい形式で提供する**
  - **一発でわかる表現形式**
  - **特に、経営層にアピールしやすい形式が求められている**

ＪＮＳＡの総合セキュリティ評価基準？

ＪＮＳＡで制定するメリット

- 中立的な立場で、基準を制定できる
  - 各社の実状を盛り込みつつ、特定の会社に依存しない
  - オープンな制定手順
- エンドユーザに結果を提示する場合に、使いやすい
  - 業界団体ということで、標準的なイメージがある
  - 中立的な団体なので、特定の会社の色が無い
- 基準そのものの信頼感（が、あると思う）
  - 一企業が策定するよりは、信頼感がある（と思っている）

ＪＮＳＡ総合セキュリティ評価基準の目標

JNSA

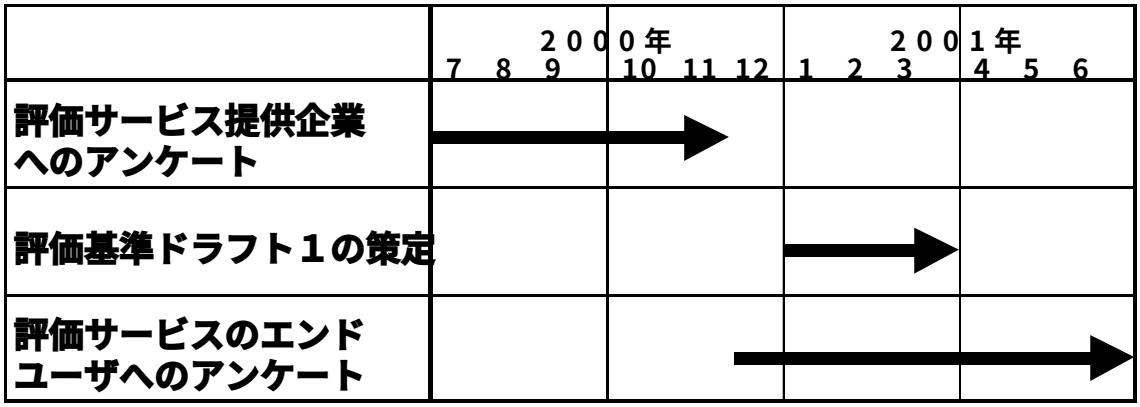
１．サーバ，もしくはシステムの、総合評価を出す

- ひとつの値，たとえば、「７５点」とか「ランクＢ＋」とか

２．具体的な検査ツール製品に関わらず、使用できる基準とする

- ISS InternetScanner だけでなく、Axent NetRecon，CyberCop Scanner でもＯＫ

評価基準作成のスケジュール



日本ネットワークセキュリティ協会
Japan Network Security Association

JNSA

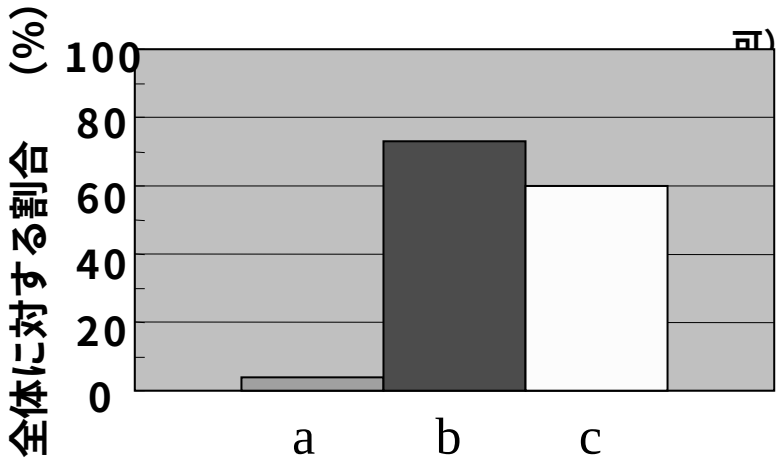
セキュリティ評価サービス
提供企業へのアンケート結果

アンケート結果

JNSA

Q.貴社にてセキュリティ検査サービスを実施している目的は？

（複数回答可）

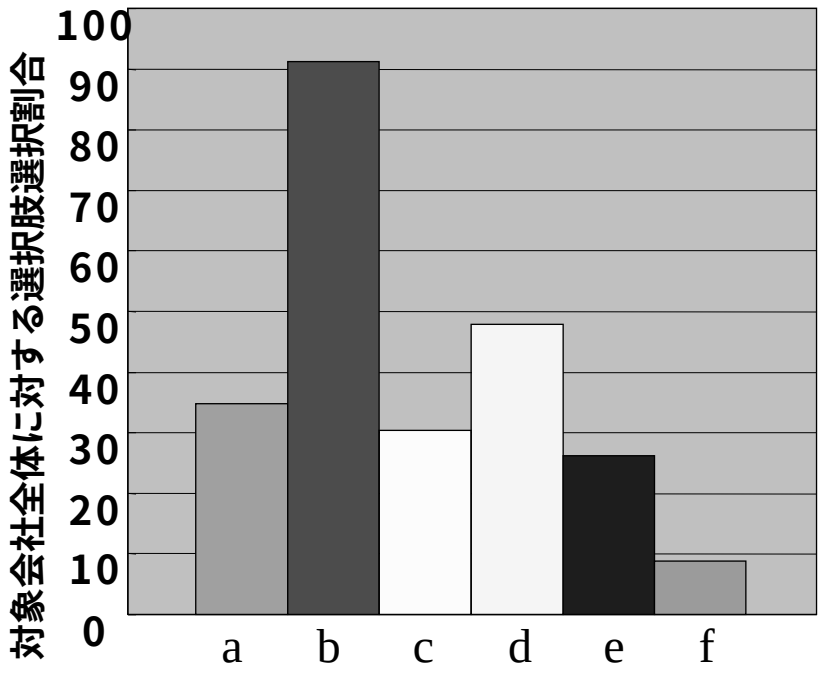


a. サービスそのもので事業が成り立つから
b. 自社にとって必要なサービスメニューだから
c. 他のビジネスにつながるから

アンケート結果

JNSA

Q.貴社で実施しているセキュリティ検査サービスは どういったものですか？



a. 問診表により主にセキュリティポリシーの制定状況や運用状況を検査するサービス

b. 市販またはフリーウェアなどのツールによりネットワークやサバの脆弱性を検査するサービス

c. 自社による独自ツールを使用しネットワークやサーバの脆弱性検査するサービス

d. 自社技術者のノウハウを使用しネットワークやサーバの脆弱性を検査するサービス

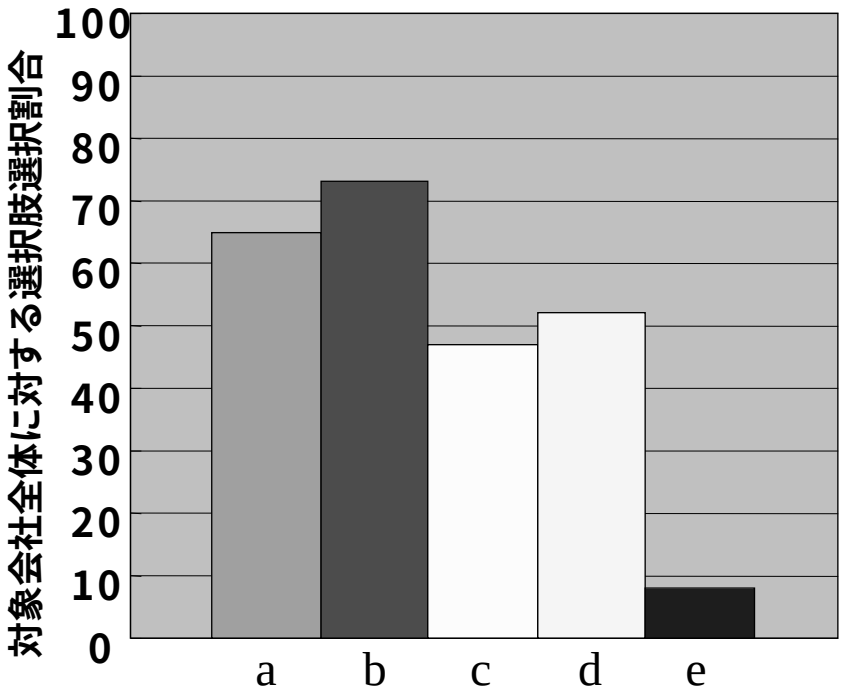
e. 他社のサービスを利用または仕入れたサービス

f. その他

アンケート結果

JNSA

Q.貴社のお客様がセキュリティ検査サービスを受ける目的は？



（複数回答可）

a. 安全性を確認するため定期的に実施している

b. 安全性を確認するために実施（定期的ではない）

c. 今後どういう対策が必要かを認識するために実施

d. 試しに実施

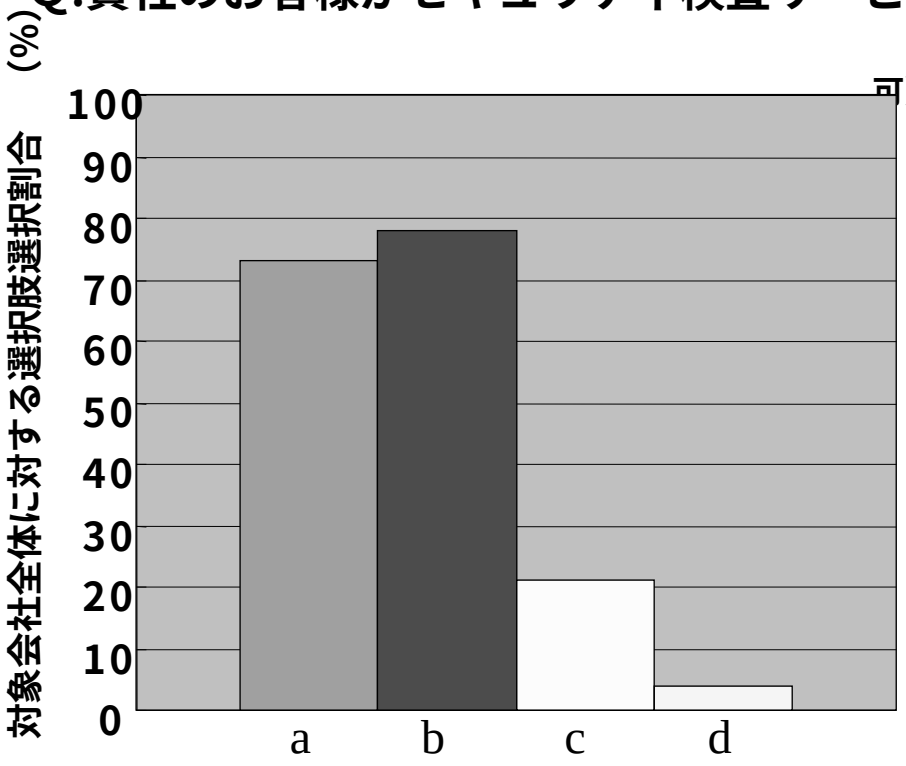
e. その他

アンケート結果

JNSA

Q.貴社のお客様がセキュリティ検査サービスを受けた感想は？

（複数回答可）

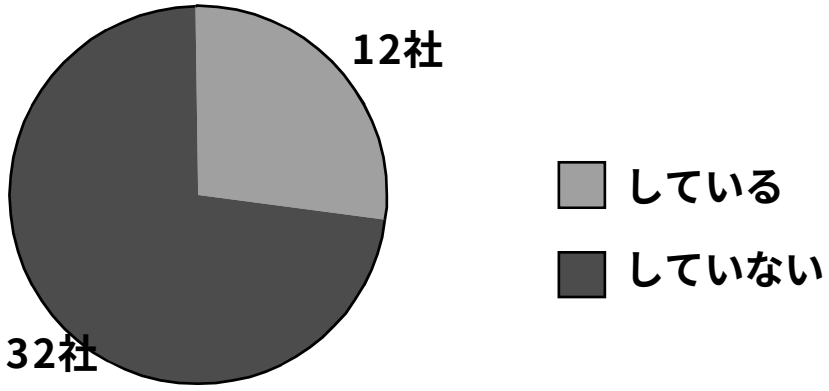


a. 満足したと思う
b. 普通だと思う
c. 不満に思っている
d. その他

アンケート結果

JNSA

Q.総合セキュリティ評価を実施していますか？

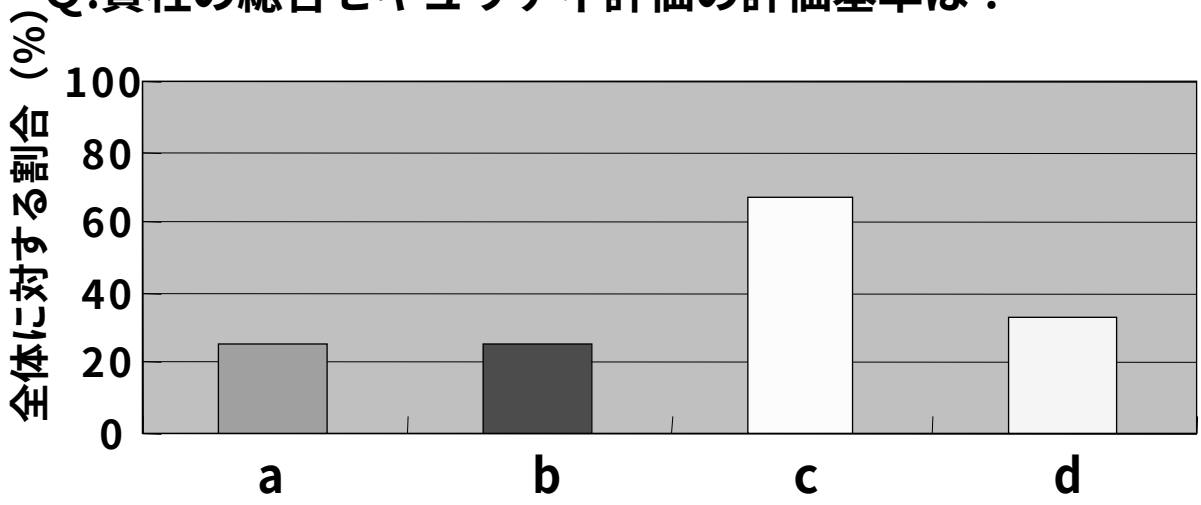


[参考] セキュリティ検査サービス実施企業：２２社

アンケート結果

JNSA

Q.貴社の総合セキュリティ評価の評価基準は？



a. 利用するツールの判定に依存

b. 明確な規定は無く担当者の判断に依存

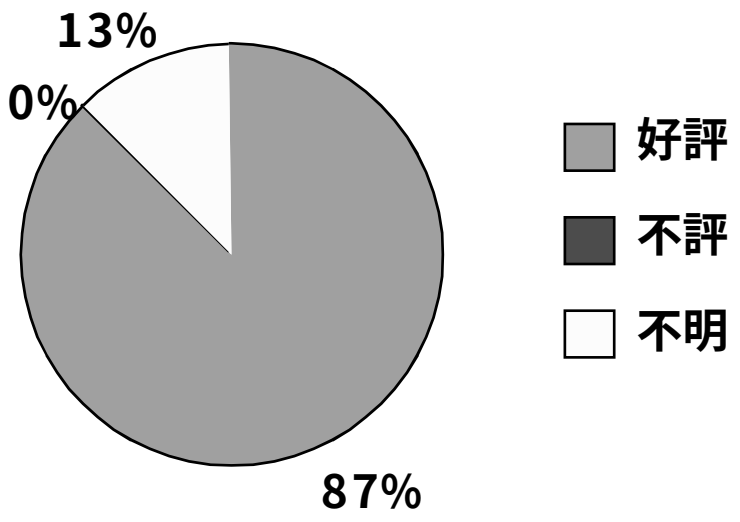
c. 自社内または他社との間に取決めた規定に従う

d. その他

アンケート結果

JNSA

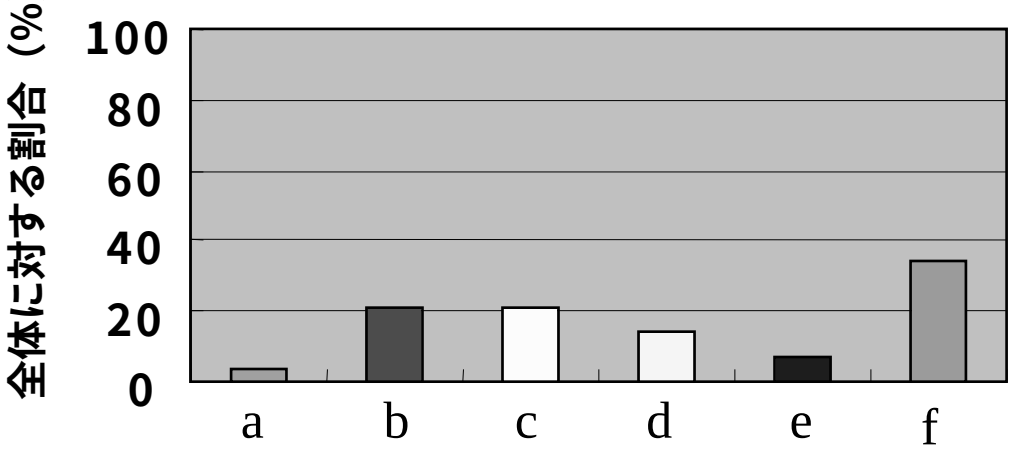
Q.総合セキュリティ評価に関する顧客の反応は？



アンケート結果

JNSA

Q.総合セキュリティ評価を実施していない場合、その理由は？

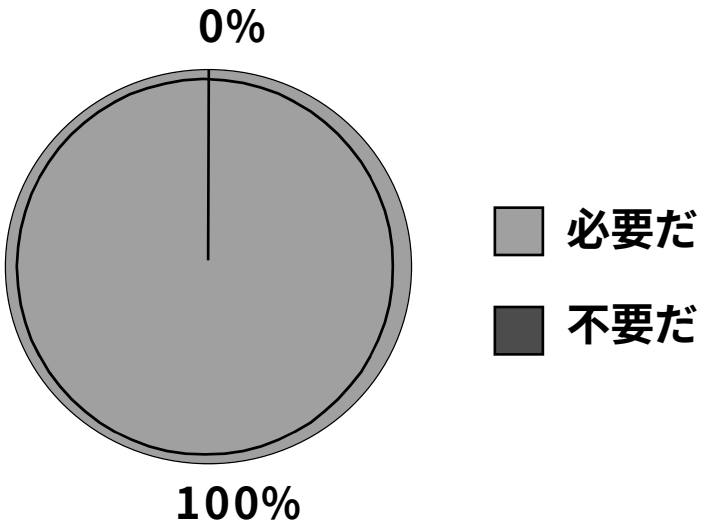


a. 必要性を感じない
b. 人手/予算的な問題
c. 技術ノウハウ不足
d. 明確な評価基準を保持していないため
e. その他
f. 無回答

アンケート結果

JNSA

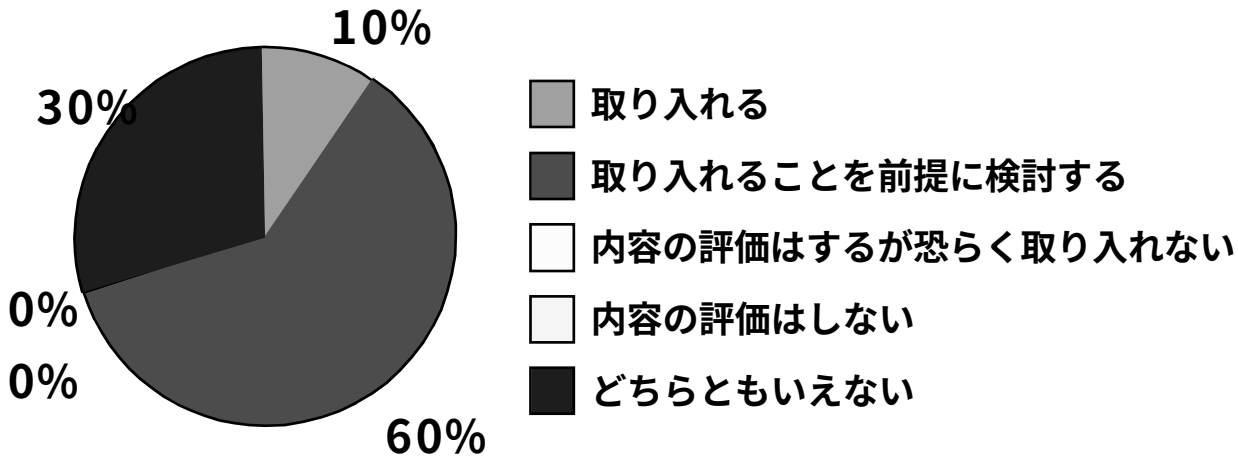
Q.総合セキュリティ評価は顧客にとって必要ですか？



アンケート結果

JNSA

Q.総合セキュリティ評価基準（ガイドライン）を公開した場合、その内容を取り入れますか？



アンケート結果のまとめ

JNSA

- 100%の企業が、お客様にとって総合セキュリティ評価は必要と考えている。
- 総合セキュリティ評価を実施している企業の90%がお客様から好評を得ている。
- 検査サービス実施企業の50%が総合セキュリティ評価を実施していない。

⇒　明確な基準が無いと答える企業が多い。

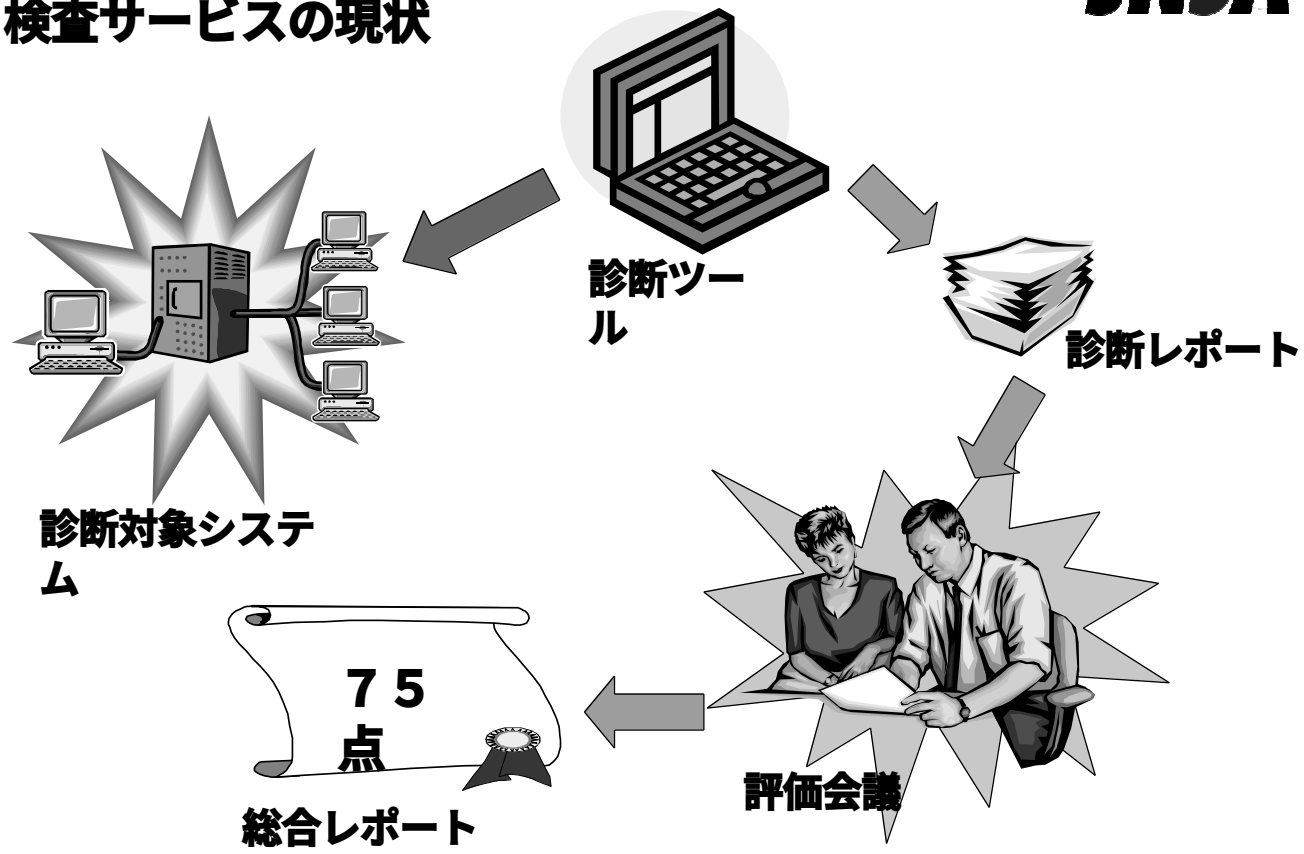
総合セキュリティ評価基準（ガイドライン）を策定することは意義がある。

日本ネットワークセキュリティ協会
Japan Network Security Association

JNSA

総合評価基準　ドラフト1

検査サービスの現状



診断ツールのレポート

JNSA

１．応答のあったポートの検出

- 応答内容によって、稼動しているプログラム（デーモン・サービス）を特定

２．いわゆる、セキュリティホールの検出

この２点を盛り込んだ、評価基準を検討

JNSA

オープンポートのセキュリティレベル検討

[議論点]

WWWサーバにおいて、80/tcp ポートがオープンしていることは脆弱性を高めていることになるのか？

[結論]

80/tcp ポートが無応答であるマシンよりも脆弱性が高いのは間違いない。だから、脆弱姓を高めていると考えられる。

[総合評価基準への適用]

各ポート（サービス）ごとに、脆弱性ポイントを設定し、その合計でセキュリティレベルを判定する１要素とする。

各ポートの脆弱性ポイント（原案）

tcp	udp	サービス	脆弱ポイント
21	---	ftp	5
22	---	ssh	4
23	---	telnet	6
25	---	smtp	5
53	53	domain	4
80	---	www	3
110	---	pop3	4
136	136	SMB	6
137	137	SMB	6
138	138	SMB	6

セキュリティホールの脆弱性ポイント（原案）

誰でも実行できる ⟷ スキルが必要

リスク ＼ 実現性	1	2	3
A	80	70	60
B	60	50	40
C	40	30	20

被害が大きい ↕ 被害が軽い

セキュリティホールの実現性

1 - 誰でもツールをダウンロードして実行することが可能

ハッカーサイトなどにツールが存在するもの

使用にあたって、技術的なスキルが必要でないもの

2 - 実現方法が公開されており、少々スキルがあれば実行可能

ハッカーサイトなどに実行方法が説明されているもの

ごく基本的なスキルがあれば、実現できるもの

3 - 実現方法は未公開であり、かなりのスキルがないと実現できない

実行の手がかりは公表されていても、具体的な方法が公表されていないもの

高度なスキルがなければ、実現できないもの

セキュリティホールのリスク

JNSA

A- リスク大

- リモートから管理者権限が取得できる
- リモートから任意のコマンドを実行できる
- リモートからファイルが改ざんできる

B- リスク中

- リモートからDoS攻撃が可能
- リモートから重要なファイルを閲覧できる
- リモートからサービスの不正使用が可能（メールのオープンリレーなど）

C- リスク小

- 一般ユーザが管理者権限を取得できる
- 一般ユーザとしてログインできる
- リモートから一般的な（想定外の）ファイルを閲覧できる

セキュリティホールのリスク（追加）

JNSA

リスク小であっても．．．

(1) リモートから一般ユーザとしてログインできる

(2) 一般ユーザが管理者権限を取得できる

上記のように連続して使用すれば、リスク大と同じくリモートから管理者権限が取得できてしまう

総合ポイントの算出

１．ポート脆弱性

- 各ポートの脆弱性ポイントを合計
- ただしシステム総合評価の場合、同一サービスが複数サーバで検出されても、１台分のみ合計対象とする

２．セキュリティホール脆弱性

- 検出されたセキュリティホールをマトリックスにあてはめて、脆弱性ポイントを合計
- ただし、同一区分のセキュリティホールが複数検出された場合、１つめのみ合計対象とする

３．総合ポイントの算出

１００ － ポート脆弱性 － セキュリティホール脆弱性

総合ポイントのガイドライン

１００～９１	クラスA
９０～７１	クラスB
７０～４１	クラスC
４０～　１	クラスD
０～	クラスE

検討点

１．ポートの脆弱性ポイント

- 上限値が必要か？　最大でも２５ポイントまでとか

２．セキュリティホールの実現性ポイントの決定

- ハッカーサイトって、どこ？
- アップデートはどうするか？

３．個別の脆弱性ポイントの決定

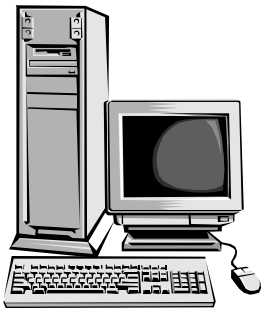
- どうやって決定していくのか？
- アップデートはどうするか？

日本ネットワークセキュリティ協会
Japan Network Security Association

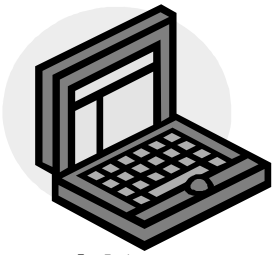
JNSA

総合評価基準 ドラフト1 の適用例

ケーススタディ： WindowsNT単独サーバ



診断対象システム
WindowsNT4.0 Server
ServicePack 6a
IIS 4.0
すべてデフォルトインストール



診断ツール
Symantec(AXENT)
NetRecon 3.0

診断レポート

総合評価基準
ドラフト１で総合評価

1．オープンポートの脆弱性ポイント

TCP

ポート	サービス	点数
139	netbios-ssn	6
80	http	3
53	domain	4
25	smtp	5
21	ftp	5

UDP

ポート	サービス	点数
53	domain	---
137	netbios-ns	---
138	netbios-dgm	---

合計	23

2．セキュリティホール脆弱性のポイント

脆弱点名	リスク	実現性	ポイント
IIS-RDS	C	1	40
InvalidExecutab Parsing	A	1	80
IndexServer DirectoryTraver	B	2	50
		合計	170

JNSA

３．総合ポイントの算出

計算式：

１００ － ポート脆弱性 － セキュリティホール脆弱性

今回の事例：

１００ － ２３ － １７０ → －９３

総合評価は、－９３ポイント，クラスＥ

セキュリティ対策を実施すると？

TCP

ポート	サービス	点数
1	Firewall でブロック	~~6~~
80	http	3
53	domain	4
25	smtp	5
21	ftp	5

UDP

ポート	サービス	点数
53	domain	---
137	netbios-ns	---
138	netbios-dgm	---

合計	~~23~~ → 17

セキュリティ対策を実施すると？

脆弱点名	リスク	実現性	ポイント
IIS-RDS	RDSの停止		~~40~~
InvalidExecutab Parsing	パッチ適用		~~80~~
IndexServer DirectoryTraver	.htwタイプ削除		~~50~~
		合計	~~170~~

→ 0

JNSA

対策後の総合ポイント

計算式：

１００ － ポート脆弱性 － セキュリティホール脆弱性

今回の事例：

１００ － １７ － ０ → ８３

総合評価は、８３ポイント，クラスＢ

日本ネットワークセキュリティ協会
Japan Network Security Association

JNSA

セキュリティ評価サービス
エンドユーザへのアンケート

総合セキュリティ評価へのアンケート

JNSA

以下のホームページ上でアンケートをお願いする予定です。ご協力をお願いいたします。

http://www.jnsa.org/

JNSA

技術部会　セキュリティ評価WG