JNSA

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

ちょっとネタ振り

情報セキュリティ対策の詳細について考える

2008年 6 月13日

JNSA 2007年度活動報告会

セキュリティ市場調査WG
グループリーダー　勝見　勉

市場の新しい動きトピックス

2007年度セキュリティ市場調査報告書より

1. 外部からの攻撃の脅威
2. 内部統制と情報セキュリティ
3. 情報セキュリティ監査
4. 情報セキュリティ対策におけるASP/SaaSの市場動向について
5. 物理的セキュリティとの連携
6. セキュリティ対策の実効性評価
   1. PCI DSS
   2. 情報セキュリティ格付け制度
   3. ISO27004と日本ISMSユーザグループの活動
   4. 情報処理推進機構の研究レポート
   5. 電子商取引推進協議会によるセキュリティ対策評価モデル
   6. 米国国立標準技術研究所（NIST）からのガイドライン（SP）

謝辞：ありがとうございました

- ＪＡＳＡ　調査研究部会ＷＧ１
  http://www.jasa.jp/seika/seika.html

- 日本ＩＳＭＳユーザグループ
  http://www.j-isms.jp/events/20071221.html

- ＪＮＳＡ市場調査WG

http://www.jnsa.org/seminar/2008/0613/index.html

セキュリティ対策の有効性評価研究

2003/7	NIST SP-800-55 Security Metrics Guide for Information Technology Systems
2004/4	IPA　**定量的セキュリティ尺度測定ガイドライン** **(「定量的セキュリティ測定手法および支援ツールの開発」調査報告書別冊)**
2005/2	ECOM　**セキュリティ対策評価モデル**
2006/9	PCI SSC　PCI DSS Payment-Card industry Data Security Standard V1.1
2006/11	BSI BIP0074:2006 Measuring the effectiveness of your ISMS implementations
2006/12	**日本**ISMS-UG　JISQ27001**管理策有効性測定に関するサンプル集**
2007/7	**情報セキュリティ格付け制度研究会**
2007/12	**日本**ISMS-UG　**メジャメント研究会活動報告**
2008/4	JASA**報告書：　保証型セキュリティ監査　・・・体系整備とガイドの作成**
2008/6	JNSA**活動成果報告会　BoF**
200?	ISO/IEC27004

NISTの刊行物

- FIPS 200 (2006/2): **連邦政府の情報および情報システムに対する最低限のセキュリティ要求事項**
- SP 800-26(2001/11): IT**システムのためのセキュリティ自己アセスメントガイド**
- SP 800-53(2005/2): **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**： Annex1,2,3: **レベル低・中・高**
- SP 800-55(2003/7): IT**システムのためのセキュリティメトリクスガイド**

出典：IPA**セキュリティセンター**
http://www.ipa.go.jp/security/publications/nist/index.html

NIST SP800-55 サンプルメトリクス

A.5 システムセキュリティ計画

重要項目	5.1 境界コントロールが効果的でない場合、システムと相互接続されている全システムについて、セキュリティ計画が文書化されていますか?
詳細質問	5.1.1 システムセキュリティ計画は主要な部門やマネジメント層に承認されていますか?
メトリクス	承認されたシステムセキュリティ計画があるシステムの割合
目的	マネジメント層が承認したシステムセキュリティ計画の度合いを測る。これには計画の完成度やその計画が該当する要件を満たしているかを暗に示すものとなる
実施証拠	1. あなたの組織は、IT システムに関する資産目録を最新の状態に維持していますか? □ はい □ いいえ 2. 「はい」と答えた場合、あなたの組織(または組織の構成部門)にはいくつのシステムがありますか? 3. 何件のシステムセキュリティ計画が完了していますか? ___ 4. NIST SP 800-18 に定められたすべてのトピックを盛り込んだシステムセキュリティ計画はいくつありますか? _____ 5. マネジメント層が承認したシステムセキュリティ計画はいくつありますか?
頻度	年 1 回
計算式	承認されたシステムセキュリティ計画の数(質問 5) ／ システムの総数
データソース	システム資産目録とシステムドキュメント追跡システム(質問 2)
指標	このメトリクスの目標は 100%である。上昇傾向を示し、100%に近づくことが望ましい。システムセキュリティ計画の完成は、OMB Circular A-130 『*Management of Federal Information Resources*』の付録 III、「Security of Federal Automated Information Resources」および公法 100-235、1987 年のコンピュータセキュリティ法で義務付けられている。システムセキュリティ計画では、システムに管理が組み込まれているか、または組み込む予定があることを明確に記述し、行動規則の一覧も説明すべきである。マネジメント層がシステムセキュリティ計画を承認することで、適切なシステムセキュリティを指示するための、システムセキュリティ計画の必須要素が完了したことになる。

出典：IPAセキュリティセンター
http://www.ipa.go.jp/security/publications/nist/index.html

IPA　定量的セキュリティ尺度測定ガイドライン

実施：㈱情報数理研究所

IPA：2003年度 電子政府情報セキュリティ技術開発事業
http://www.ipa.go.jp/security/fy15/development/metrics/index.html

- **考え方のソースは**NIST
- SP800-26　SP800-55**を参照して具体的に展開**

参考情報

表 2　組織的な IS の測定のタイプ

準拠性評価	定義された組織活動があり、測定ではその定義にしたがって準拠していることを計測する。 測定は、静的に近い。 測定は、比較的容易である。
有効性、妥当性評価	評価対象の有効性、妥当性を測定する為には、精査が必要である。 測定は動的であり、多岐に渡る。 測定は“準拠性評価”に比べて、桁違いに難解なものとなる。

出典：IPAセキュリティセンター

表 1 に、NIST SP 800-26 再録されている“連邦 IT セキュリティ評価フレームワーク”（前年出された基準文書）に示されている 5 段階評価を記す。評価基準として、5 段階のそれぞれに 3－6 程度の細目の評価基準が示されており、整備された成熟度指標となっている。

表 1 「連邦 IT セキュリティフレームワーク」での成熟度指標

レベル 1	文書化されたポリシー
レベル 2	文書化された手続き
レベル 3	手続きの実行と管理
レベル 4	試験されレビューされた手続きと管理
レベル 5	完全に統合された手続きと管理

IPA　定量的セキュリティ尺度測定ガイドライン(2)

定量化尺度の定義フォーマット

表 3　定量化尺度定義様式

目標	定量的尺度での測定対象となっているシステムセキュリティコントロール項目の目的/技術を実装する場合の望ましい結果を記述したもの。NIST SP 800-26 を用いる場合は、この項目はある重要要素(Critical Element)に対応する。
詳細目標	上記の目標を達成するために必要な行動を記述したもの。NIST SP 800-26 を用いる場合は、この項目は目標の下位にあたる 1 つまたは複数の質問に対応する。
尺度	定量測定の見地から尺度を定義したもの。「パーセント」「数」「頻度」「平均値」といった用語を含む数値を記述する文である。
尺度の目的	定量的尺度の結果を収集することで得られる全ての作用を記述したもの。組織内部での性能測定に用いるのか組織外部への報告に使用されるのかの区分、ある定量的尺度から得られる所見、また特定の測定を求める社会的規制や法律（そういうものがあるとして）、また、その他の同様の項目を含む。
実装の証拠	セキュリティコントロールの実装を証明する存在証拠を列挙したもの。実装の証拠は、活動が行われたことを示す間接指標として、またはある特定の定量的尺度が不満足な結果となった場合の原因を示す要素として、定量的尺度の計算のために使用される
頻度	経時的に変化するデータの測定を行うデータ収集の時間間隔を示したもの。コントロールの実装で生じる更新の期間に関係する。
計算式	定量的尺度の数値結果を示すための計算式を記述したもの。実装証拠を集めた情報は、定量的尺度の計算式の入力情報として扱われる。
出所	定量的尺度の計算に用いるデータの場所を示したもの。データベース、追跡ツール、組織、必要な情報を提供できる組織の特定の役職などを含む。
指標	定量的尺度の意味とその値の傾向についての情報を提供するもの。測定結果の変化傾向の原因と、観察された欠陥を解決する方法とを示唆する。定量的尺度の測定値の目標範囲が既に設定されている場合はそれを記述する。また、測定値の目標範囲の視点から見て、どのような値の変化傾向が肯定的なものであるかを述べる。
関連性	SSE-CMM のプロセスエリアとの関連性の定義 情報セキュリティ監査制度の管理基準との関連性の定義

出典：IPAセキュリティセンター

IPA　定量的セキュリティ尺度測定ガイドライン(3)

定義フォーマットにより定義展開したメトリクスの項目

1) 情報資産の定期的なリスクの見直し率
2) 環境変化が生じた時のリスクの見直し率
3) リスク評価で発見された脆弱性の対策立案率
4) リスク評価で計算された年間予想被害額
5) リスク評価について関係者が結果を確認した割合
6) ビジネス特性からの被害（インパクト）分析の検討率
7) セキュリティテストの実施率
8) 弱点発見から解決までの平均所要日数
9) ライフサイクル計画における機密度設定
10) システムライフサイクルにしたがったセキュリティ投資
11) 調達前にセキュリティテストが行われた実施率
12) システム管理者のコモンクライテリアの認識率
13) 変更管理における試験結果の文書化率
14) 開発後セキュリティコントロール変更時の再承認率
15) マシン相互接続時に正式に承認手順を取る割合
16) 正式な認証を受けていないシステムの稼働率
17) システムセキュリティ計画の所属長による承認率
18) システムセキュリティ計画の定期見直し率
19) 責任･権限が適切に複数の人に分離されている割合
20) 無効アカウントの残存率
21) 機密データ操作要員の選考･訓練の実施率
22) アクセスコントロールの評価の実施率
23) 要員の選別での補完
24) 記憶媒体の貸し出し管理実施率
25) モニタ画面の盗み見対策の実施率
26) 通信施設の収容所に対する入退室管理の実施率
27) モニタ画面、机の上が整理されている割合
28) モバイル機器の機密データの暗号化率
29) モバイル機器の持ち出し管理実施率
30) 未解決問題に対するヘルプデスクからのサポート率
31) 文書、および電子文書における機密度の設定の遵守率
32) 記憶媒体を廃棄、再利用する時の完全消去率
33) バックアップの実施率
34) コンティンジェンシープランのリカバリー責任者の任命率
35) コンティンジェンシープランの訓練実施率
36) コンティンジェンシープランのテスト実施率
37) 外部委託によるシステム保守要員の操作制限の実施率
38) システム変更時の再承認率
39) 不要なシステムプログラムの稼動状況の点検率
40) パッチがインストールされていることの追跡調査率
41) ウィルス対策ソフトの最新パターンのダウンロード率
42) ウィルス対策ソフトの自動スキャン率
43) パスワード設定におけるパスワードポリシーの遵守率
44) 侵入検知ツールの導入率
45) 購入アプリケーションのマニュアルの整備率
46) 開発アプリケーションの文書化維持率
47) システム毎のリスク評価の文書化維持率
48) セキュリティ要員へのトレーニング実施率
49) インシデント対応態勢の組織内での保有率
50) インシデント情報の組織内の共有化率
51) 事故通報義務の遵守率
52) デジタル証明書の導入率
53) 暫定ユーザIDの削除率
54) パスワードの定期変更の実施率
55) 暗号強度を把握しているシステムの割合
56) バイオメトリクスの認識エラー率を把握している割合
57) 不十分なパスワード管理の発見率
58) ユーザID を共有している割合
59) セキュリティ対策ソフトウェアの権限者以外アクセス
60) 定期的なプロトコルの調査実施率
61) ネットワークログの調査分析率
62) ネットワークログの平均保存月数
63) プライバシーポリシーのウェブサイトへの適用率
64) Web サイト構築時のクロスサイトスクリプティング対処率
65) 操作コマンド、ファイルアクセスログの記録率

出典：IPAセキュリティセンター

ECOM　セキュリティ対策評価モデル

出典：ECOM　次世代電子商取引推進協議会
METI：2004年度 ブロードバンドセキュリティに関する調査研究
http://www.ecom.or.jp/results/results16.html

対策要求の体系：　ISMS管理策体系?

参考１　：表 2-2　ECOM セキュリティ対策評価モデルにおける対策要求の体系

ビュー	サブ・ビュー	対策ドメイン	要求対策数
マネジメント・ビュー	セキュリティ対策推進基盤の確立	セキュリティマネジメント環境の整備	6
		経営レベルでのセキュリティ要求の明確化(注)	3
	セキュアな組織運営と業務の運営の実現	組織管理上でのセキュリティ対策	3
		業務運営上でのセキュリティ対策	4
		業務現場における情報の保護の徹底	4
		ユーザ管理の徹底	2
		法的要求事項の遵守	3
テクニカル&オペレーショナル・ビュー	システムの信頼性の確保	システムの処理の正確性の確保	5
		障害に対する堅牢性の確保	3
		システムの性能の確保	5
	攻撃に対する堅牢性の確保	不正アクセス対策	12
		セキュリティホール対策	4
		ウィルス対策	4
		システム情報および セキュリティ管理情報の保護	3
		システム上の業務情報の保護	4
		通信路上の情報の保護デジタル情報の長期有効性の確保	3
		インターネットサービスの利用における対策	2
		サービス妨害への備え	2
		システムの動きに対する監視の実施	3
	セキュアなシステムの構築とその維持	セキュアなシステムの構築とその維持	2
		ソフトウェアの管理の徹底	3
		個々の機器における自衛策の実施	3
		セキュアなアプリケーションソフトの開発	3
		システム運用上のセキュリティ対策	6
	システムの安全とセキュアなシステム運用の実現	保管電子情報の有効性の確保	4
		特殊な利用環境に対するセキュリティ対策	8
		施設や設備の保護	3
		セキュリティ事故への備え	5
アシュアランス・ビュー	セキュリティ対策の実施の評価	監査手法による対策状況のチェック	3
		技術診断によるセキュリティ対策の欠陥のチェック	2

(注) リスク分析を含む

ECOM　セキュリティ対策評価モデル(2)

対策強度レベルの定義　成熟度モデルと通ずる?

参考２：ECOMのセキュリティ対策評価モデルに対策強度レベルの設定基準

レベル区分	強度レベルの概念
レベル5	● 問題が生じる余地は、まず、ないと考えることができる理想とするレベル。ただし、実施には相当の負担がともなう。 当該対策要求について、それが技術的な要求の場合は、現時点で考えられる最高水準の技術の採用や対策の２重化等が、また、現場の実務や管理面についての要求の場合には、不手際が発生する余地をほとんどなくすとともに、不手際が発生してもそれをカバーする仕組みや、問題を見逃さないようにする仕組みが完備され、これらが完全に機能していると見なすことができるレベル。
レベル4	● ベースラインより一段と強。一般に求められるレベルより一段と高いレベルで、通常では問題が生じる可能性はほとんどなく、意図的な攻撃に対してもある程度堅牢と見ることができるレベル 当該対策要求について、それが技術的な要求の場合は、一般的なシステムが平均的に用いている技術より１ランク信頼性の高いものが使われるか、平均的技術でも平均以上に最適化が図られている。また、現場の実務や管理面についての要求の場合には、不手際が発生する余地をほとんどなくすとともに、平均的なシステムよりきめ細かいルールが策定され、またその運用が厳格に管理されており、これらが機能していることについて高い信頼がおけるレベル。
レベル3	● ベースライン。一般に求められるレベル。日常的に問題が生じる可能性は低いが、偶発的なトラブルの可能性は残り、意図的な攻撃に対しては、必ずしも十分とは言えないレベル 当該対策要求について、それが技術的な要求の場合は、平均的なシステムで一般に使用されているツール等が平均的な使われ方をしている。また、現場の実務や管理面についての要求の場合には、平均的な対応がある程度の組織的な管理の下で行われており、対策が機能していることが、相当程度の信頼できる。
レベル2	● ベースライン以下。一般的には不十分とみなされるが，リスクが低いと判断されたり，他の対策によってカバーされていること等で、当該システムではおおむね十分と判断できる場合でのみ許容できるレベル レベル３の要求については満足できないが、当該対策要求に対して、ある程度有効と思われる対策が機能していると認められるレベル。組織的な対応とは言えなくても、相当の実効性が期待できるレベル。
レベル1	● 必要最低限に達しないレベルで、実施はしえちるもののその有効性は期待できないレベル

出典：Ecom 次世代電子商取引推進協議会

PCI DSS: カード業界データセキュリティ基準

要求条件 (要件) の体系

出典：JCBグローバル　http://www.jcb-global.com/pci/index.html

安全なネットワークの構築・維持
要件1：カード会員データを保護するためにファイアウォールを導入し、最適な設定を維持すること
要件2：システムパスワードと他のセキュリティ・パラメータにベンダー提供のデフォルトを使用しないこと

カード会員データの保護
要件3：保存されたカード会員データを安全に保護すること
要件4：公衆ネットワーク上でカード会員データを送信する場合、暗号化すること

脆弱性を管理するプログラムの整備
要件5：アンチウィルス・ソフトウェアを利用し、定期的に更新すること
要件6：安全性の高いシステムとアプリケーションを開発し、保守すること

強固なアクセス制御手法の導入
要件7：カード会員データへのアクセスを業務上の必要範囲内に制限すること
要件8：コンピュータにアクセスする利用者毎に個別のID を割り当てること
要件9：カード会員データへの物理的アクセスを制限すること

定期的なネットワークの監視およびテスト
要件10：ネットワーク資源およびカード会員データに対するすべてのアクセスを追跡し、監視すること
要件11：セキュリティ・システムおよび管理手順を定期的にテストすること

情報セキュリティ・ポリシーの整備
要件12：情報セキュリティに関するポリシーを整備すること

PCI DSS: カード業界データセキュリティ基準(2)

要求条件 (要件) の個別要求事項の記述例

1.1 以下を含むファイアウォール設定基準を確立する。
1.1.1 すべての外部ネットワーク接続とファイアウォール設定の変更を、認可・テストするための正式な手順。
1.1.2 無線ネットワークを含む、カード会員データへの全接続を示す最新のネットワーク図。
1.1.3 すべてのインターネット接続、およびDMZ (demilitarized zone) **と内部ネットワーク領域との間にファイアウォールを必ず置くこと。**
1.1.4 ネットワーク・コンポーネントの論理的管理のためのグルーピングと、それぞれの役割や責務に関する記述。
1.1.5 業務に必要なサービス／ポートの文書化されたリスト。
1.1.6 HTTP (hypertext transfer protocol)、SSL (secure sockets layer)、SSH (secure shell)、VPN (virtual private network) **以外で利用可能なプロトコルが存在する場合、その必要性の正当な理由とそれを記した文書。**
1.1.7 危険性のあるプロトコル (例：FTP=file transfer protocol**) を許可する場合の正当化理由と文書。そこにはそのプロトコルの利用理由と、実装されるセキュリティ機能が含まれる。**
1.1.8 ファイアウォール／ルータに関するルール・セットの四半期レビュー。
1.1.9 ルータの設定基準。

出典： VISA International Tokyo
http://www.visa-asia.com/ap/jp/merchants/riskmgmt/includes/uploads/zantei.pdf

PCI DSSの特徴／注目点

https://www.pcisecuritystandards.org/
http://www.jcb-global.com/pci/index.html
http://www.visa-asia.com/ap/jp/merchants/riskmgmt/includes/uploads/zantei.pdf

- 要求が具体的
- 実効ある対策を要求

- 評価基準が具体的(?)

- 「守る」目的が明確かつ単一

日本ISMSユーザグループのメジャメント研究

JISQ27001管理策有効性測定に関するサンプル集（例）-1

A.10.4.1　悪意のあるコードに対する管理策　（1/2）

2006年度セミナー発表

目的	A.10.4　悪意のあるコード及びモバイルコードからの保護 ソフトウェア及び情報の完全性を保護するため
管理策	A.10.4.1　悪意のあるコードに対する管理策 悪意のあるコードから保護するために、検出、予防及び回復のための管理策、並びに利用者に適切に意識させるための手段を実施しなければならない
検討ポイント	内容
①脅威	悪意のあるコードの侵入
②脆弱性	a悪意のあるコードの侵入経路となりうる外部記録媒体・Web閲覧・メールおよびその添付ファイル等の取り扱いに対する啓発・教育・注意喚起の不徹底 b悪意のあるコードからの対策ソフトの未導入 c悪意のあるコードからの対策ソフトの定義ファイルのアップデート未実施 d悪意のあるコード検知時の対応手順の不備
③リスク	a外部記録媒体の利用ルールやWeb閲覧の制限、メールやその添付ファイルの取り扱いルールがない、又は不徹底であったことに起因する悪意のあるコードの侵入 b悪意のあるコードからの対策ソフトの未導入・定義ファイル未更新による悪意のあるコードの侵入 c悪意のあるコード侵入時の不適切な対応による悪意のあるコードの侵入拡大
④管理策の目的、目標	＜目的＞ a悪意のあるコードの侵入経路を利用者に意識させ、悪意のあるコードが侵入するリスクを低減する。 b悪意のあるコードからの対策ソフトを確実に導入し、悪意のあるコードが侵入するリスクを低減する。 c定義ファイルを常に最新の状態に保つことにより、悪意のあるコードが侵入するリスクを低減する。 d組織内の利用者に悪意のあるコードに関する教育や啓発活動を実施することにより、悪意のあるコードの侵入および侵入拡大のリスクを低減する。 ＜目標＞ a目的を達成するための実装された管理策の100%実施 b実装された管理策の対象となるリスクに関連した、リスク受容水準を超えるインシデントの発生0%

19

http://www.j-isms.jp/events/20071221.html

出典：日本ISMSユーザグループ

日本ISMSユーザグループのメジャメント研究(2)

JISQ27001管理策有効性測定に関するサンプル集（例）-2

2006年度セミナー発表

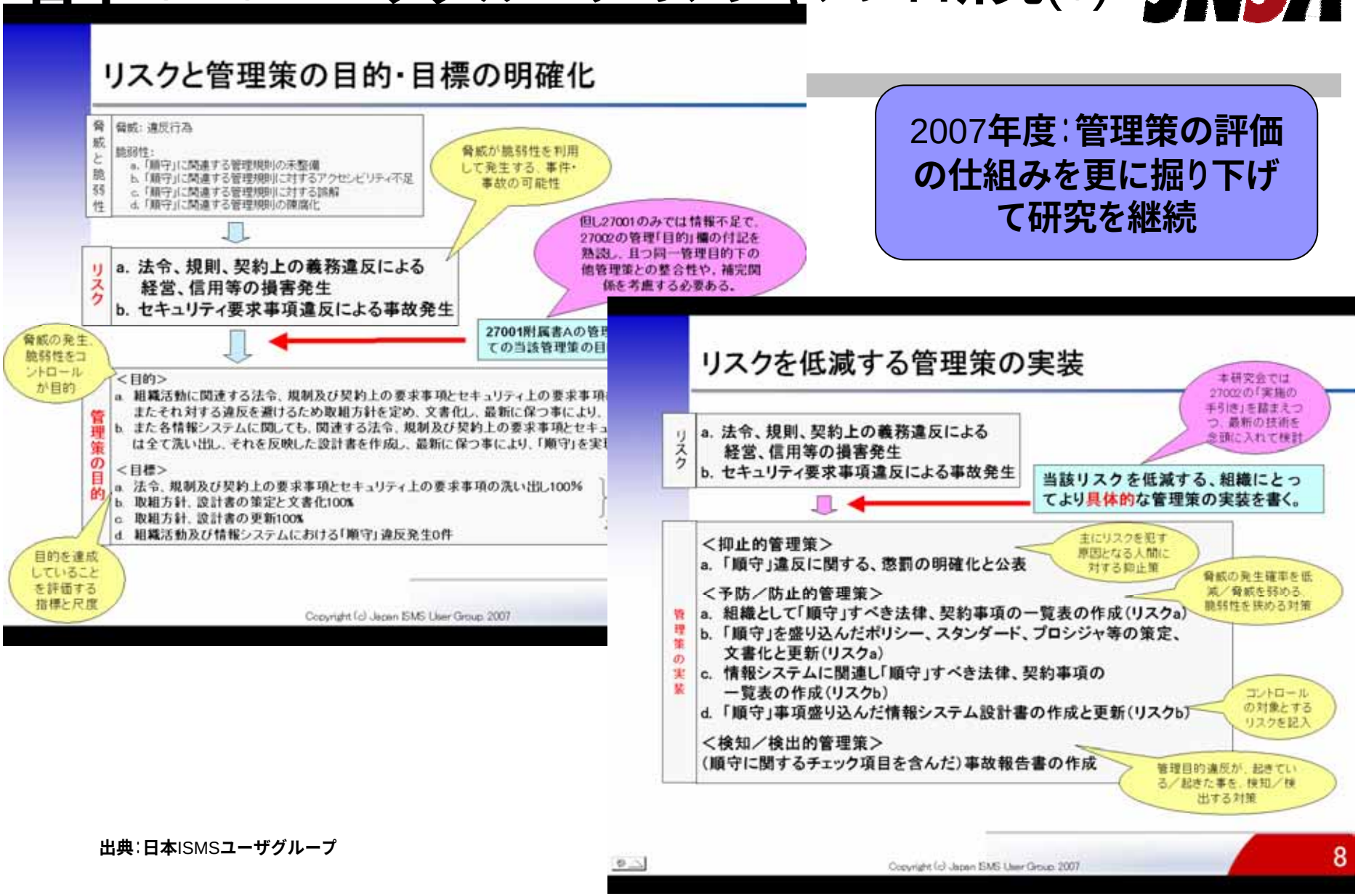
A.10.4.1　悪意のあるコードに対する管理策　(2/2)

⑤管理策の実装	管理策実装の事例： ＜抑止的管理策＞ ＜予防/防止的管理策＞ a.外部記録媒体の利用制限 b.不要なWebサイトの閲覧制限 c.組織内ネットワークのサーバやクライアント端末への悪意のあるコード対策ソフトの導入 d.導入した悪意のあるコード対策ソフトのパターンファイルのタイムリーな更新 e.許可されていないソフトウェアの使用制限 f.組織内の利用者に対する悪意のあるコードに関する教育・啓発活動の実施 g.悪意のあるコード侵入時の拡大防止・駆除の手順の確立 ＜検知/検出的管理策＞ a.悪意のあるコードに関する情報の収集および警戒情報の組織内展開 b.電子メールやインターネット、媒体等により外部から入手したファイルの使用前の、悪意のあるコードのスキャン
⑥有効性測定方法	（今回は未記入）
⑦管理策のタイプ	実施要求
備考	電子メール経由で伝送される悪意のあるコードについては、A.10.8.1でも情報交換の方針および手順を備えるよう、要求されている。 スパムメール・Dos・ボットは、A.10.8.4（サービスの可用性）、セキュリティパッチの適用については、A.12.6.1で考慮することとし、本管理策では考慮しない。 モバイルコードは、悪意のあるコードとは別物と考える。 フィッシングは、犯罪行為であり、管理策で対応するものではない。A.8.2.2の情報セキュリティの意識向上・教育で考慮する。

20

出典：日本ISMSユーザグループ

日本ISMSユーザグループのメジャメント研究(3)



2007年度：管理策の評価の仕組みを更に掘り下げて研究を継続

出典：日本ISMSユーザグループ

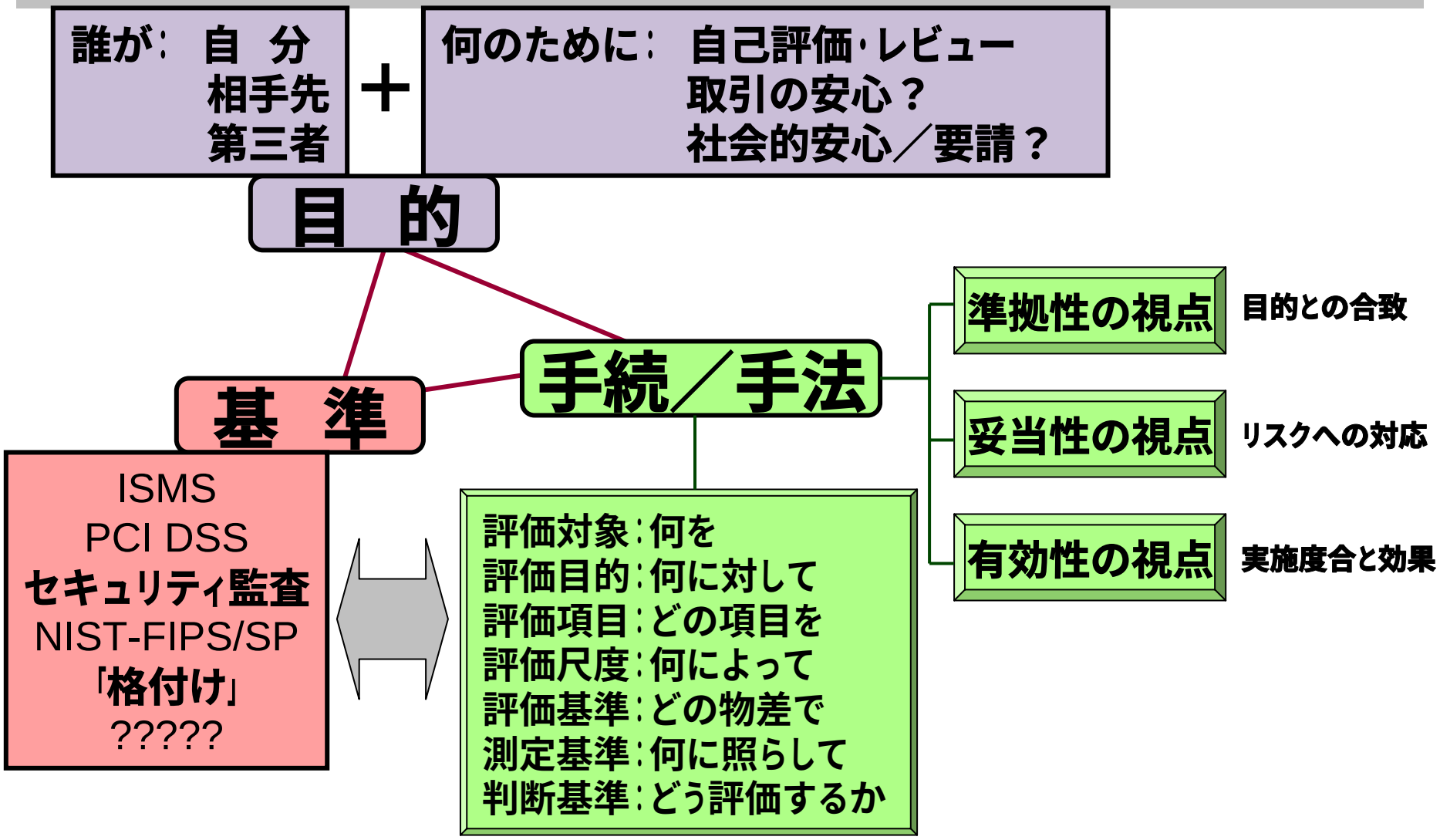
保証型情報セキュリティ監査

JASA：日本セキュリティ監査協会

http://www.jasa.jp/kansa/wframework/index.html
http://www.jasa.jp/seika/seika.html

- 「保証」を目的とした情報セキュリティ監査
  VS 「助言型」
- 「目的」と「対象」と「基準」で3類型
  - 被監査主体合意方式：　委託元→委託先
  - 利用者合意方式：　委託先→委託元
  - 社会的合意方式：　委託先→一般社会
- 監査基準と監査手続の選択により、セキュリティ対策の「有効性」評価の有力手段に

セキュリティ対策の有効性評価：ディスカッションの切り口として



Let's Talk/Chat/Discuss!

http://www.jnsa.org
sec@jnsa.org