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

「業務に基づく中小企業の情報セキュリティ対策ガイドライン」作成についてのご報告

元持哲郎
アイネット・システムズ株式会社
JNSA西日本支部

2011年 1月25日

概　要

西日本支部では、２００４年に開始した中小企業向け個人情報保護WG活動をステップとして、中小企業向けにセキュリティ対策のガイドラインとして「情報セキュリティチェックシート」を作成しました。

さらに2009年3月より、中小企業向を対象にした、業務に基づくリスク分析・評価・対応・対策方法を検討し作業してきました。

今回は、2年間の作業結果を中小企業が負担に感じる事無く実践できるアプローチとして作成した「業務に基づく中小企業の情報セキュリティ対策ガイドライン」について概説致します。

ガイドラインの目的

- 情報の洗い出し無でセキュリティ対策が可能
- 対象とする中小企業に業務に伴うリスクが判別できる
- 対象とする中小企業が具体的なリスク対策が行える
- 対策を継続的に行っていける

ガイドラインの構成

- 導入部
  - 1.概要
  - 2.本ガイドライの対象企業
  - 3.本ガイドラインの対象読者
  - 4.本ガイドラインの使用方法
- 第1部
  - 18の情報セキュリティ管理項目
- 第2部
  - 62業務に基づく情報セキュリティ対策例
- 付録
- 参考資料

対象の企業

従業員300人以下

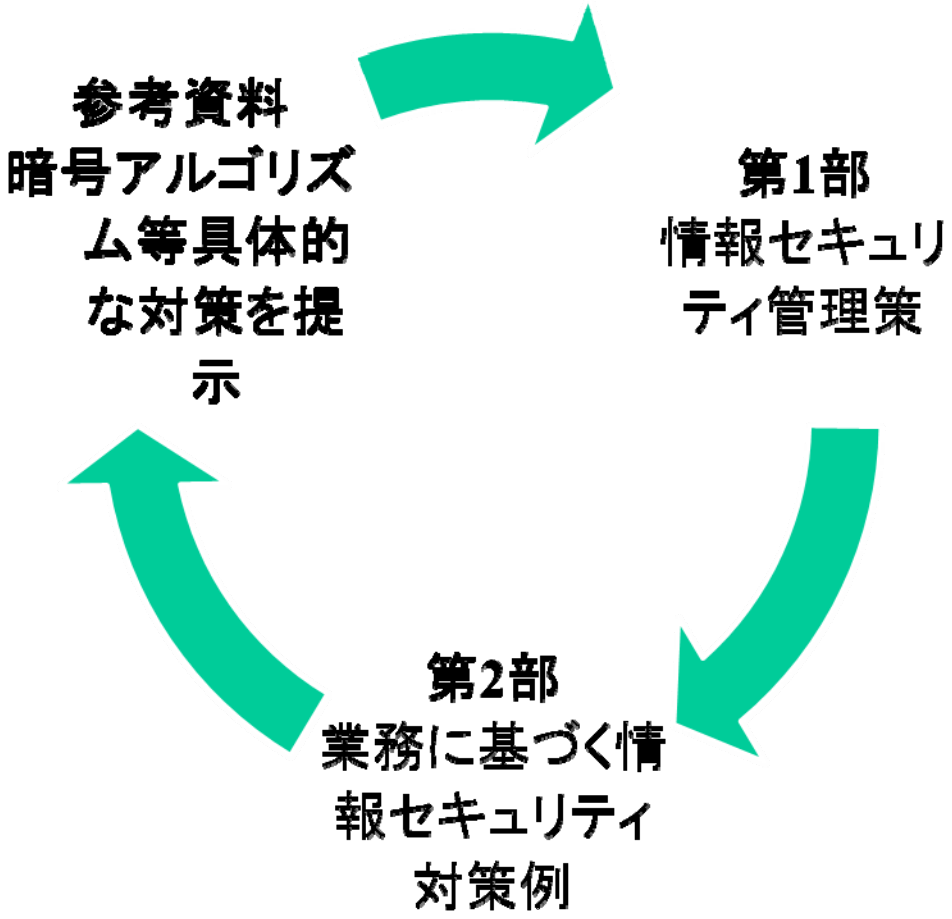
分類群	企業分類	情報セキュリティの意識	対策の要請	管理レベル
Ⅰ	取引先からの要請に応える事が求められる企業 （大手企業との取引のウエイトが高い企業）	◎	企業規模に拘わらず委託元と同等の水準を求められている。	ISMS、プライバシーマーク
Ⅱ	責任の明確化・職務の分類が行われている企業 （自社の情報セキュリティ対策が必要な企業）	○	企業価値向上・内部統制等目的から対策する事の必要に迫られている。	本ガイドライン
Ⅲ	責任の明確化・職務分類が行われていない企業	△	守るべき情報資産があり、守らねばならない必要意識が漠然とはあるが、費用対効果が見えず躊躇・逡巡し、対策の実践が伴わない。	
		×	情報セキュリティ対策の必要を感じない。	

西日本支部 2008年度活動成果物「中小企業の情報セキュリティ対策支援 WG活動報告書」より

対象読者

- 企業のシステム管理者
- システム管理を外注している管理者

使用方法



ガイドライン第1部

- 1.セキュリティ境界と入退室管理
- 2.認証と権限
- 3.ウイルス及び悪意のあるプログラムに対する対策
- 4.パッチの適用
- 5.バックアップ　☆
- 6.ログの取得　☆
- 7.記憶媒体の管理
- 8.暗号化
- 9.アプリケーションの利用

ガイドライン第1部

- 10.電子メールの利用
- 11.外部サービスの利用
- 12.ネットワークのアクセス制御
- 13.クリアデスク・クリアスクリーン
- 14.変更管理　☆
- 15.構成管理　☆
- 16.障害・事故管理　☆
- 17.容量・能力の管理　☆
- 18.Webの開発・管理

管理策から省いた項目

- 対象が紙・物に関するもの
- 電源、空調等の設備管理に関するもの
- 対策できないもの、対策が中小企業レベルでは難しいもの
  - 経営者、システム管理者等の権限者の不正
  - DoS攻撃
- 個人情報保護に関するもの
- 委託管理に関するもの
- 対策が教育・啓蒙になるもの

ISMSとの対応

本ガイドライン管理項目	ISMS-ISO/IEC27001:2005-付属書A　対応管理策
1.セキュリティ境界と入退室管理	A.9.1.1,A.9.1.2
2.認証と権限	A.11.2.1,A11.2.2,A.11.2.4,A.11.5.1,A.11.5.2,A.11.5.3,A.11.6.1
3.ウイルス及び悪意のあるプログラムに対する対策	A.10.4.1,A10.4.2
4.パッチの適用	A.12.6.1
5.バックアップ	A.10.5.1
6.ログの取得	A.10.10.1,A.10.10.2,A.10.10.3,A.10.10.4,A.10.10.5,A.10.10.6
7.記憶媒体の管理	A.10.7.1,A10.7.2
8.暗号化	A.12.3.1,A.12.3.2
9.アプリケーションの利用	
10.電子メールの利用	A.10.8.4
11.外部サービスの利用	A.10.2.1
12.ネットワークのアクセス制御	A.11.4.2,A.11.4.3,A.11.4.5,A.11.4.6,A.11.4.7
13.クリアデスク・クリアスクリーン	A.11.3.3
14.変更管理	A.10.1.2,A12.5.1
15.構成管理	A.7.1.1,A.12.4.1
16.障害・事故管理	A.13.1.1,A.13.1.2,A.13.2.2
17.容量・能力の管理	A.10.3.1
18.Webの開発・管理	A.10.9.1,A.10.9.2,A10.9.3

第1部 9.アプリケーションの利用

(1)管理目的

アプリケーションの利用に伴う、情報の漏えい、改ざんから情報を保護するため

(2)管理策

①有償、無償を問わず組織が許可したソフトウエアのみを使用する

②大きな脆弱性の存在が明らかなファイル共有ソフト、P2P(Winny、Share等)の使用は禁止する

③電子ファイルを外部に提供する必要がある場合は、情報そのもの以外に、ファイルのプロパティ、ヘッダー、フッターにある情報も確認し外部に公開すべきでない情報は消去する

④プレゼンテーションソフトを使用し外部に提案を行う場合は、PCのデスクトップ上にある外部に公開すべきでない情報は見えないようにする

⑤登録機能を使用してFAX送信する場合にも、登録間違いによる誤送信を防止するために宛先番号を確認して送信する

⑥FAX送信する場合は、送信前に送信相手に、送信することの連絡、送信後に受信確認を行う

⑦重要な情報を保存する場合は、後に情報の重要度及び属性が容易に判断可能なようにファイル名を命名する

(3)運用で心がけるポイント

①無許可ソフトがユーザPCにインストールされていないか定期的に棚卸を実施する

(4)関連する管理項目

認証と権限、ウイルス及び悪意のあるプログラムに対する対策、暗号化

ガイドライン第2部

- 出社　　1業務
- 社内業務　　31業務
- 社外業務　　12業務
- 退社　　1業務
- 帰宅　　2業務
- システム管理業務　15業務

ガイドライン第2部

業務 No.123	業務名
情報を処理・保存するための実体	□建物・部屋・エリア　□キャビネット　□机上　□PC　□サーバー □ネットワーク　□アプリケーション　□記憶媒体(USBメモリー他) □プリンター　□FAX　□コピー機　□携帯電話　□電子機器(ICレコーダー、カメラ他)　□外部のサービス（ファイル交換サービス等)
影響	□機密性　□完全性　□可用性　□適法性
脅威の要因	□システム管理者(本人)　□システム管理者(本人外)　□従業員(本人) □従業員(本人外)　□訪問者　□外部　□偶発的要因
責任者	□システム管理者　□業務・人事管理者　□従業員
セキュリティの対策の目的	

ガイドライン第2部

現状のセキュリティレベル	
リスクシナリオ	
技術的対策	
人的対策	
運用で心がけるポイント	
備考	

関連する管理策：

「第1部」と「第2部」との対応

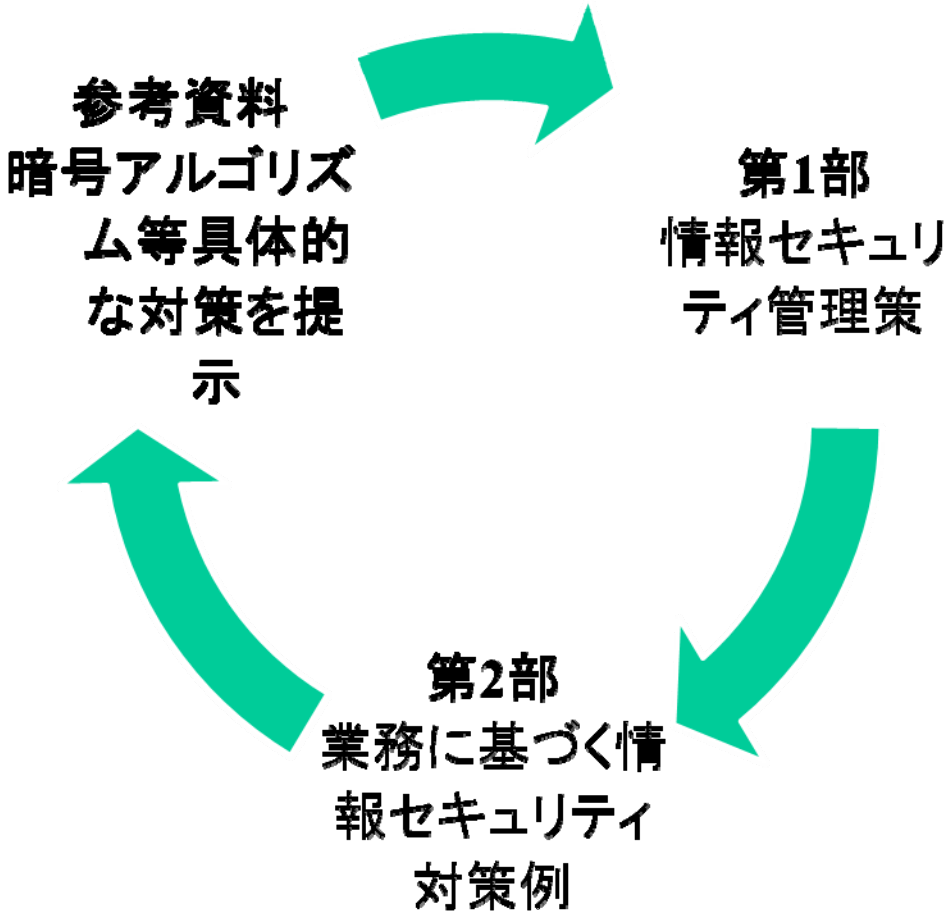
第1部		第2部
本ガイドライン管理項目	管理策	業務No.
1.セキュリティ境界と入退室管理	①	1,2,22,28,57
	②	1,2,22,28
	③	3
2.認証と権限	①	1,4,12,21,28,35,41,42,46
	②	4,21,42
	③	1,2,3,5,21,42
	④	1,2,21
	⑤	21
	⑥	6
3.ウイルス及び悪意のあるプログラムに対する対策	①	7
	②	7
	③	13,58
	④	13,58
	⑤	25
	⑥	25
	⑦	58
4.パッチの適用	①	8,60
	②	
5.バックアップ	①	9,23,50
	②	9,23,48,49,50
	③	23,50
6.ログの取得	①	3,55
	②	54
	③	55
	④	55
	⑤	
7.記憶媒体の管理	①	12,38,40
	②	32
	③	
	④	11
	⑤	
8.暗号化	①	14,16,20,35,38,39,40,44,46
	②	
	③	14,16,20
9.アプリケーションの利用	①	47
	②	47
	③	19
	④	37
	⑤	17
	⑥	17
	⑦	20

第1部		第2部
本ガイドライン管理項目	管理策	業務No.
10.電子メールの利用	①	
	②	15
	③	14,16
	④	14
	⑤	
11.外部サービスの利用	①	24,26
	②	
12.ネットワークのアクセス制御	①	36,59,61
	②	59,61
	③	42,43
	④	59,61
	⑤	59,61
	⑥	31
	⑦	30,31,57
	⑧	25
13.クリアデスク・クリアスクリーン	①	45
	②	27,33,34,45
	③	29
	④	18
14.変更管理	①	48
	②	48
	③	48
	④	48
	⑤	49
	⑥	49
15.構成管理	①	10,51
	②	51
	③	
16.障害・事故管理	①	53
	②	52
	③	52
17.容量・能力の管理	①	56
	②	56
18.Webの開発・管理	①	62
	②	59
	③	59,61
	④	61
	⑤	61

強度・程度のわかる参考資料を紹介

- パスワードポリシー
- 暗号リスト
- データ消去
  - 物理的
  - 理論的
- SaaS SLA
- Web開発

各部の関係



Sample1 2 認証と権限

(1)管理目的

情報と情報機器への許可されていないアクセスを防止するため

(2)管理策

①入館・入室設備、PC(BIOS,OS)、サーバー、ネットワーク、アプリケーション、携帯電話等にアクセスするための個人及びプログラムを認証する仕組みを構築・設定する

②認証には、IDカード、デバイス(ICカード、USBキー等)、パスワード、バイオメトリックス(指紋認証、静脈認証等)等の、第三者が簡単に利用できない仕組みを用いる

③認証のためのユーザIDは個人を特定できるように付与する

④ユーザIDは職務権限に応じた、情報と情報機器へのアクセス権限を付与する

⑤特権は、システム管理者、業務の管理者等特別の職務権限を持った者だけに付与する

⑥パスワード[9]は例えば「8文字以上に設定し、
大文字、小文字、数字、特殊文字の4つを組み合わせ、
3カ月に1度変更する」
(以降「」をパスワードポリシーとする)とする。

(3)運用で心がけるポイント

①退職、人事異動に伴う、ユーザID、権限の見直しを行う

②特権は初期設定のAdministratorは使用せず、システム管理者の個別ユーザIDに特権を付与する

Sample 1

第1部		第2部
本ガイドライン管理項目	管理策	業務No.
1.セキュリティ境界と入退室管理	①	1,2,22,28,57
	②	1,2,22,28
	③	3
2.認証と権限	①	1,4,12,21,28,35,41,42,46
	②	4,21,42
	③	1,2,3,5,21,42
	④	1,2,21
	⑤	21
	⑥	6
3.ウイルス及び悪意のあるプログラムに対する対策	①	7
	②	7
	③	13,58
	④	13,58
	⑤	25
	⑥	25
	⑦	58

Sample 1

業務 No.6	PC の起動・ログイン
情報を処理・保存するための実体	□建物・部屋・エリア　□キャビネット　□机上　■PC　□サーバー □ネットワーク　□アプリケーション　□記憶媒体(USB メモリー他) □プリンター　□FAX　□コピー機　□携帯電話　□電子機器(ＩＣレコーダー、カメラ他)　□外部のサービス（ファイル交換サービス等)
影響	■機密性　□完全性　□可用性　□適法性
脅威の主体	□システム管理者(本人)　□システム管理者(本人外)　□従業員(本人) ■従業員(本人外)　□訪問者　□外部　□偶発的要因
責任者	■システム管理者　□業務・人事管理者　■従業員
セキュリティの対策の目的	情報と情報機器への許可されていないアクセスを防止するため
現状のセキュリティレベル	簡単なパスワード(数字 4 桁など)を使用している

Sample 1

リスクシナリオ	簡単なパスワードを使用しているためログオン時の覗き見によりパスワードが漏えいし、情報にアクセスされる
技術的対策	認証システムのパスワードポリシーを設定(複雑なパスワード、定期的パスワードの変更) し、ユーザに強制的にパスワードポリシーを使用させる
人的対策	パスワードの文字数、文字列の組み合わせ、変更の周期等についてのパスワードポリシーをルール化しユーザに周知徹底する
運用で心がけるポイント	・認証システムのパスワードポリシーを確認する ・パスワードルールが周知徹底されているかユーザに確認する
備考	

関連する管理策：2.認証と権限 ⑩

Sample 1

(9)Japan Vulnerability Notes

「共通セキュリティ設定一覧CCE概説 (パスワード編)」

http://jvndb.jvn.jp/apis/myjvn/cccheck/cce_password.html

Sample1

設定に関するセキュリティ項目には、Windows XPとWindows Vista毎に、CCE識別番号が割り当てられています。推奨値は、基準とするセキュリティ設定ガイドによって決まります。ここでは、米国国防情報システム局(DISA)、米国連邦政府共通デスクトップ基準(FDCC: Federal Desktop Core Configuration)、ならびに、マイクロソフトのセキュリティ設定ガイドで推奨されている値を示します。

表1. パスワード関連項目を対象としたCCE識別番号と推奨値

CCE-ID		セキュリティ項目	セキュリティ設定ガイド		
XP	Vista		DISA(*a)	FDCC(*b)	マイクロソフト
CCE-2981-9	CCE-2883-7	パスワードの最低文字数設定 (パスワードの長さ)	14文字以上	12文字以上	8文字以上
CCE-2920-7	CCE-2967-8	パスワードの有効期間	60日以下	60日以下	90日以下
CCE-2994-2	CCE-2323-4	パスワードの履歴管理 (同じパスワードを連続して使えない回数)	24個以上	24個以上	24個以上
CCE-2439-8	CCE-3240-9	パスワードの変更禁止期間	1日以上	1日以上	1日以上
CCE-2986-8	CCE-3177-3	ログオンできなくなるまでのパスワード入力失敗回数(アカウントのロックアウトのしきい値)	3回以内	5回以内	50回以内
CCE-2466-1	CCE-2715-1	パスワード入力失敗回数のリセットまでの期間 (ロックアウトカウントのリセット)	60分以上	15分以上	15分以上
CCE-2928-0	CCE-2363-0	ログオン不可状態からの復旧時間 (ロックアウト期間)	ロックアウト期間を永久	15分以上	15分以上
CCE-2980-1	CCE-3050-2	スクリーンセーバーが起動するまでの時間 (スクリーンセーバーのタイムアウト)	15分以下	15分以下	-
CCE-4500-5	CCE-4290-3	パスワード付きスクリーンセーバー	要設定	要設定	-

「共通セキュリティ設定一覧CCE概説 (パスワード編)」

Sample 2　7.記憶媒体の管理

(1)管理目的

情報の漏えい、改ざん、消去、破壊を防止するため

(2)管理策

①記憶媒体の数量、所在を管理する

②使用した記憶媒体(ハードディスク、テープ、USBメモリー、CD、DVD、スマートカード等)を廃棄する場合は、保存した情報が解読できないように、信頼できる方法で、記憶媒体の物理的破壊(10)、情報の磁気的な消去または上書き消去(11)を行う

③重要な情報を保存した記憶媒体は、製造者の仕様に従って、適切な環境(磁気、湿度、温度などの制限)及びセキュリティの確保(耐火金庫、施錠管理)できる場所に保存する

④許可されていない記憶媒体の使用ができないように、PC、サーバーのデバイス制御を行う(参考)

⑤バックアップデータを記憶媒体に長期保管する場合は、記憶媒体の寿命を考慮し、定期的に、バックアップデータを新規記憶媒体に移動する等適切な処置を行う(参考)

(3)運用で心がけるポイント

①定期的に記憶媒体の棚卸を実施し、数量、所在を確認する

②理論的にデータ消去した場合は、廃棄前に情報を消去したことを確認する

(4)関連する管理策

ウイルス及び悪意のあるプログラムに対する対策、バックアップ

Sample 2

第1部		第2部
本ガイドライン管理項目	管理策	業務No.
6.ログの取得	①	3,55
	②	54
	③	55
	④	55
	⑤	
7.記憶媒体の管理	①	12,38,40
	②	32
	③	
	④	11
	⑤	
8.暗号化	①	14,16,20,35,38,39,40,44,46
	②	
	③	14,16,20

Sample 2

業務 No.32	ＰＣ・記憶媒体の廃棄・処分
情報を処理・保存するための実体	□建物・部屋・エリア　□キャビネット　□机上　■PC　□サーバー □ネットワーク　□アプリケーション　■記憶媒体(USBメモリー他) □プリンター　□FAX　□コピー機　□携帯電話　□電子機器(ＩＣレコーダー、カメラ他)　□外部のサービス（ファイル交換サービス等）
影響	■機密性　□完全性　□可用性　□適法性
脅威の主体	□システム管理者(本人)　□システム管理者(本人外)　□従業員(本人) □従業員(本人外)　□訪問者　■外部　□偶発的要因
責任者	■システム管理者　■業務・人事管理者　■従業員
セキュリティの対策の目的	情報の漏えい、改ざん、消去、破壊を防止するため
現状のセキュリティレベル	PC、記憶媒体の廃棄手順を定めていない

Sample 2

リスクシナリオ	PC、記憶媒体の情報が不完全な消去状態（OS でデータを削除しただけ）で廃棄されたため情報が復元され漏えいする
技術的対策	・読み取りができないように物理的破壊を行う ・データ消去ツールを使い、データを上書きする
人的対策	廃棄業者に廃棄処分を依頼し、廃棄した旨を証明するマニフェストを取得する
運用で心がけるポイント	データをツール等で消去した場合は、作業が確実に終了したことを確認する(PC が起動できない等)
備考	PC のデータは OS の機能を使用し削除しただけでは、ツールを使用し容易にデータの復元が可能である

関連する管理策：7.記憶媒体の管理 ②

Sample 2

(10)社団法人　電子情報技術産業協会

「パソコンの廃棄・譲渡時におけるハードディスク上のデータ消去に関する留意事項」

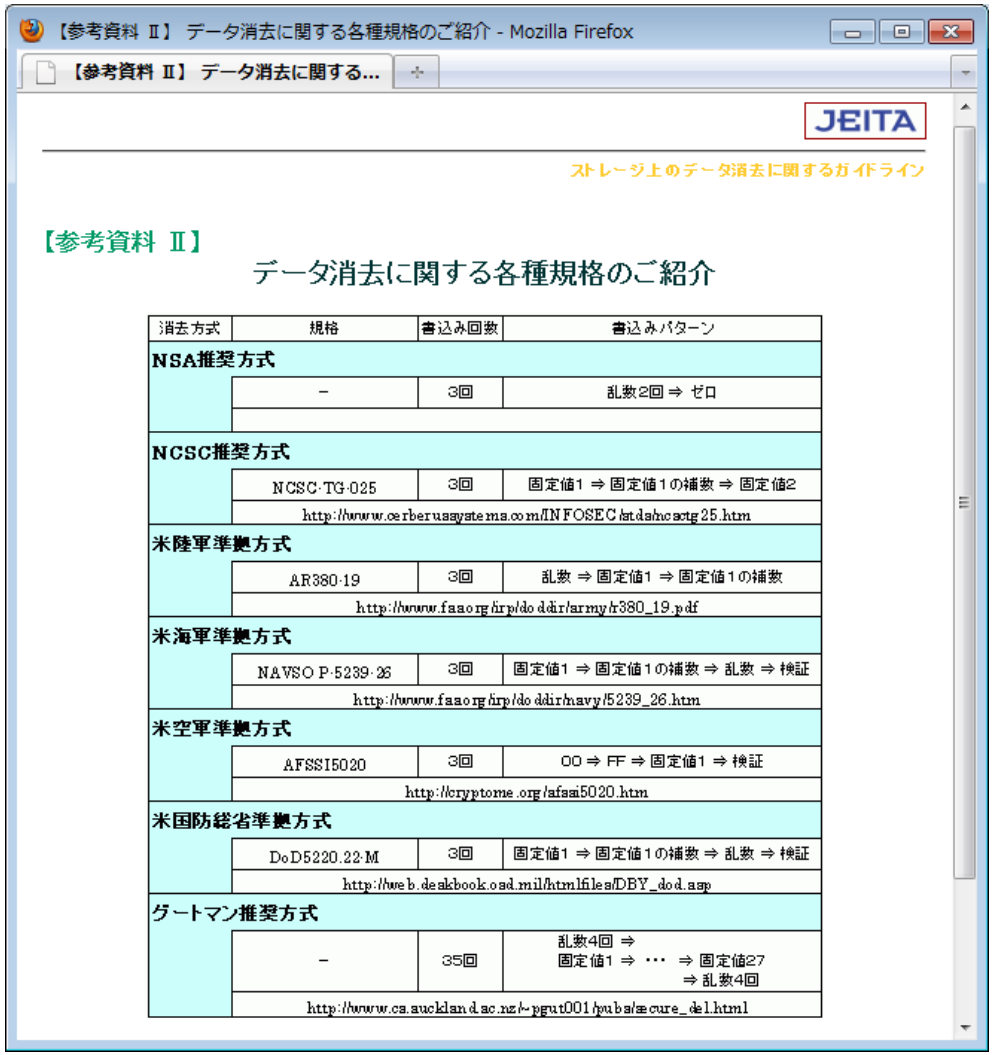
http://it.jeita.or.jp/perinfo/committee/pc/JEITA_HDDdata100219F.pdf

(11)社団法人　電子情報技術産業協会

「データ消去に関する各種規格のご紹介」

http://it.jeita.or.jp/infosys/committee/network/guideline0407/standard.html

Sample 2



消去方式	規格	書込み回数	書込みパターン
NSA推奨方式			
	-	3回	乱数2回 ⇒ ゼロ
NCSC推奨方式			
	NCSC-TG-025	3回	固定値1 ⇒ 固定値1の補数 ⇒ 固定値2
	http://www.cerberussystems.com/INFOSEC/stds/ncsctg25.htm		
米陸軍準拠方式			
	AR380-19	3回	乱数 ⇒ 固定値1 ⇒ 固定値1の補数
	http://www.faa.org/irp/doddir/army/r380_19.pdf		
米海軍準拠方式			
	NAVSO P-5239-26	3回	固定値1 ⇒ 固定値1の補数 ⇒ 乱数 ⇒ 検証
	http://www.faa.org/irp/doddir/navy/5239_26.htm		
米空軍準拠方式			
	AFSSI5020	3回	00 ⇒ FF ⇒ 固定値1 ⇒ 検証
	http://cryptome.org/afssi5020.htm		
米国防総省準拠方式			
	DoD5220.22-M	3回	固定値1 ⇒ 固定値1の補数 ⇒ 乱数 ⇒ 検証
	http://web.deskbook.osd.mil/htmlfiles/DBY_dod.asp		
ガートマン推奨方式			
	-	35回	乱数4回 ⇒ 固定値1 ⇒ … ⇒ 固定値27 ⇒ 乱数4回
	http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html		

社団法人　電子情報技術産業協会
「データ消去に関する各種規格のご紹介」

課題

- 実際の事件・事故に基づき対策例を提示
- クラウドサービス利用に特化して対策例を提示
- スマートフォン、タブレットなど新しいデバイスへの対応

WGメンバ

50音順、敬称略

-浅野　二郎		
-礒元　芳昭		株式会社OSK
-宇佐川　道信		パナソニック電工株式会社
-大財　健治		株式会社ケーケーシー情報システム
-久保　寧		富士通関西中部ネットテック株式会社
-小柴 宏記		株式会社ケーケーシー情報システム
-斎藤 聖悟		株式会社インターネットイニシアティブ
-嶋倉　文裕		富士通関西中部ネットテック株式会社
-田口　智子		株式会社 ラック
-宮下 勝彦		ヒューベルサービス株式会社
-元持　哲郎	WGリーダ	アイネット・システムズ株式会社
-近畿経済産業局地域経済部　情報政策課		
-井上　陽一		JNSA顧問・西日本支部長

ご清聴ありがとうございました。