



INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

「暗号技術」と「暗号の利用者の視点」

IPA 技術本部 セキュリティセンター
暗号グループ
神田

- 「システム」や「製品」として「セキュア」であるためには

暗号アルゴリズムが安全



一番、基盤になるものですから



実装物が安全



穴が開いてては意味ないよね



制度・仕組みが安全



何が“Trust”？



運用管理 = リテラシがしっかり



鍵をほったらかしてはダメだよ

■ 2000年以前は「標準的な暗号」というのがなかった

- 「武器」扱い & 厳格な輸出管理(輸出規制)
「標準化対象外(署名のみ標準化対象)」
日本では「米国政府標準暗号が使えない」

■ 国内では暗号が「玉石混交」の時代

- 「自称安全」な暗号もたくさん
- セキュリティを守るためには「暗号は秘匿すべきもの」

■ 暗号研究者はマニアック・・・？

- 暗号解読手法(差分解読法、線形解読法、TMTO法、
数対篩法、・・・)に強い暗号がいいといわれても・・・



CRYPTRECが評価して「**お墨付き**」を与えます

➡ 「(旧)電子政府推奨暗号リスト」

■ 国際標準暗号の策定

- 2001年 FIPS 197 AESが発行
- 2005年 ISO/IEC国際標準暗号規格が発行
- IETFなどでも実装必須暗号は米国政府標準暗号中心へ



■ 輸出規制が大幅に緩和

- 日本は無制限・無条件に米国政府標準暗号が利用可能

■ 暗号製品環境の変化

- 暗号部分のブラックボックス化(= 自社で暗号を実装しない)

■ インターネット普及に伴う暗号の「社会的基盤化」

- “囲い込み重視”から“相互接続重視”への転換
- 米国政府標準暗号は世界中特許無償で利用可能

暗号ビジネスでは利用する**暗号アルゴリズムの集約化**が進む

新しいICRYPTREC暗号リストが公表 (1)



- 2013年3月1日、総務省・経済産業省よりリリース

電子政府推奨暗号リスト

暗号技術検討会及び関連委員会(「CRYPTREC」)により、安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、**当該技術の利用を推奨**するもののリスト

技術分類		名称	技術分類		名称
公開鍵暗号	署名	DSA	ハッシュ関数	SHA-256	
		ECDSA		SHA-384	
		RSA-PSS(注1)		SHA-512	
		RSASSA-PKCS1-v1_5(注1)	暗号利用モード	CBC	
	守秘	CFB			
		RSA-OAEP(注1)		CTR	
鍵共有	DH			OFB	
	ECDH			CCM	
共通鍵暗号	64ビットブロック暗号(注2)	3-key Triple DES(注3)	認証付き秘匿モード	GCM(注4)	
	128ビットブロック暗号	AES		メッセージ認証コード	
		Camellia		CMAC	
	ストリーム暗号	KCipher-2		HMAC	
			エンティティ認証	ISO/IEC 9798-2	
				ISO/IEC 9798-3	

新しいCRYPTREC暗号リストが公表 (2)



推奨候補暗号リスト

CRYPTRECにより安全性及び実装性能が確認され、**今後、電子政府推奨暗号リストに掲載される可能性のある**暗号技術のリスト

技術分類		名称
公開鍵暗号	署名	該当なし
	守秘	該当なし
	鍵共有	PSEC-KEM(注5)
共通鍵暗号	64ビットブロック暗号(注6)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
	128ビットブロック暗号	CIPHERUNICORN-A
		CLEFIA
		Hierocrypt-3
		SC2000
	ストリーム暗号	Enocoro-128v2
		MUGI
		MULTI-S01(注7)
ハッシュ関数		該当なし
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード	該当なし
メッセージ認証コード		PC-MAC-AES
エンティティ認証		ISO/IEC 9798-4

運用監視暗号リスト

実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなった暗号技術のうち、互換性維持のために継続利用を容認するもののリスト。
互換性維持以外の目的での利用は推奨しない。

技術分類		名称
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5(注8)(注9)
	鍵共有	該当なし
共通鍵暗号	64ビットブロック暗号	該当なし
	128ビットブロック暗号	該当なし
	ストリーム暗号	128-bit RC4(注10)
ハッシュ関数		RIPMD-160
		SHA-1(注8)
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード	該当なし
メッセージ認証コード		CBC-MAC(注11)
エンティティ認証		該当なし

(注8)「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」を踏まえて利用すること。

(注9)SSL 3.0 / TLS 1.0, 1.1, 1.2で利用実績があることから当面の利用を認める。

(注10)128-bit RC4は、SSL (TLS 1.0以上)に限定して利用すること。

(注11)安全性の観点から、メッセージ長を固定して利用すべきである。

新しいICRYPTREC暗号リストができました

暗号技術検討会
事務局:総務省、経済産業省

暗号技術評価委員会
事務局:NICT, IPA

「暗号技術の安全性評価を中心とした技術的な検討課題」を担当

暗号技術活用委員会
事務局:IPA, NICT

「セキュリティ対策の推進、暗号技術の利用促進及び産業化を中心とした暗号利用に関する検討課題」を担当

でもね・・・最近、つくづく思うこと・・・

**暗号技術の安全性議論が
どんな影響を与えているのだろうか？**

「暗号解読」の実体はどうなってるの？

- 理論的な解読手法が見つかったケース
 - ⇒ ほとんど暗号研究者だけの領域。実害はまずない
- 計算機能力の向上に伴う安全性低下のケース
 - ⇒ 予測はほとんど外れない
- トライ & エラーができる解読計算量に低下したケース
 - ⇒ 暗号に興味を持つ優秀なプログラマーも参加。攻撃力大幅アップ
- プロトコル設計に問題があるケース
 - ⇒ 高度な暗号解読しなくても、もともとのデータがわかることもある
- 実アプリケーション / プロトコルが攻撃されるケース
 - ⇒ 実害が懸念される環境が整う

「暗号学界がいう安全性」= “将来”への予防措置
「ビジネスサイドがいう安全性」= “現時点”での実害対処

- ステークホルダ間でリスク認識が異なる
 - 暗号の脆弱性による「具体的被害」が発覚した事例がほとんどなく、具体的なリスクが共有されない
 - セキュリティリテラシの格差が大きい
- 暗号世代交代へのモチベーションは一般的に高くない
 - 対応しても効果が実感できるわけではない
 - 表面上問題がなければ対策を取るデメリットのほうが強調
 - どんな暗号を使っているかはほとんど気にしていない



結局のところ、技術の話ではなく、実ビジネスに具体的影響が出るかどうか、移行を進めるかどうかのモチベーションの源

暗号世代交代のモチベーションは？

使っている暗号よりも安全性や処理性能がより良い暗号ができた

➡ たぶん違う。もし影響するなら、もっと頻繁に移行が起きているはず

現在使っている暗号が解読された(破れた)

➡ 可能性はゼロではないが…。多くの場合、特定の条件下での話なので、影響があったとしても特定の関係者だけ

現在使っている暗号を利用した製品を買ってもらえなくなった

➡ **使っている暗号が安全かどうかに関係なく影響甚大**

使っている暗号
アルゴリズムの
安全性が低下した

対処しないと悪影響
が生じることは明らか

「2010年末に
移行完了」という
移行期限を切った

対処する / しないによる影響
は必ずしも明確ではない

移行に必要な標準化・
規格化が進展した

移行に必要な製品開発の
機運が高まった

業界団体等で移行計画
策定の機運が高まった

「暗号解読」の実体はどうなってる

こっちのほうがはるかに
問題なのだが...

■ 暗号実装に問題があるケース

⇒ 実害が発生する原因としては、直接的な暗号解読よりもリスクがはるかに高い

■ 運用管理上 / 暗号設定上の問題があるケース

⇒ 暗号が正しく動くための前提条件の崩壊。利用者が管理しえない領域の問題であることも多い

■ リテラシーに問題があるケース

⇒ なりすましの危険性。リテラシーが低い人ほど対策を取らない可能性が高い

■ モラルに問題があるケース

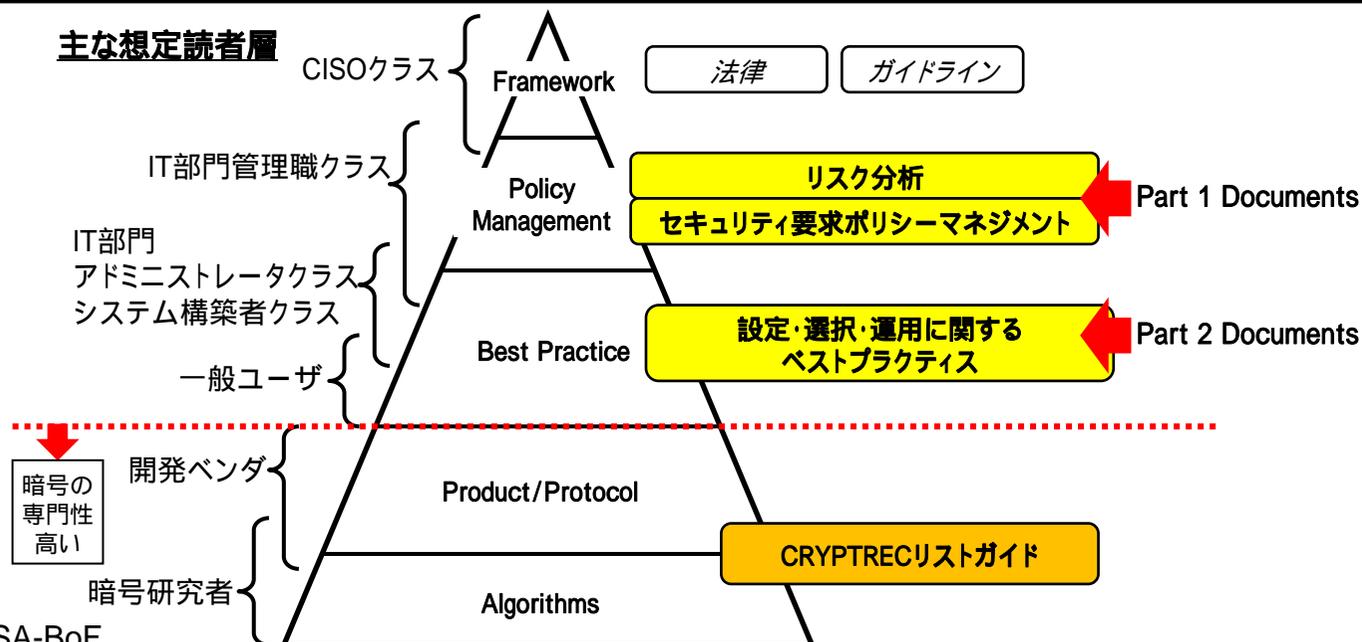
⇒ 権限自体は正規に持っているユーザが不正行為を働く。暗号だけではまず守りきれない

なぜ暗号利用マニュアルを作ろうと思ったか？

- 個人情報などの情報管理において暗号の利用は極めて有効な手段
- 適切に情報管理するには暗号に関する利用方法についての知識が必要
 - ✓ 暗号の専門家ではない人にその種の知識を持ち合わせていることを期待するのは非常に難しいのが現実
- 可用性を無視した管理規定導入と、ルール違反隣り合わせの運用が恒常化

結果として、暗号を用いた情報管理が適切に行われていないことも多い

暗号の専門家ではない人向けの暗号利用方法の単純な解説を作ろう



なぜ暗号利用マニュアルを作ろうと思ったか？



はじめは「個人情報保護ガイドライン」での参考資料化を目指した

■ 個人情報の保護に関する法律第20条

- 取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために**必要かつ適切な措置**(組織的、人的、物理的及び技術的な安全管理措置)を講じなければならない
- 本人の個人データが漏えい、滅失又はき損等をした場合に**本人が被る権利利益の侵害の大きさを考慮**し、事業の性質及び個人データの取扱状況等に**起因するリスクに応じ、必要かつ適切な措置**を講じる

【ガイドラインFAQ】

79	個人データが漏えい等したが、本人の権利利益が侵害されておらず、今後も権利利益の侵害の可能性がない又は極めて少ないと考えられるため、「影響を受ける可能性のある本人への連絡」や、「事実関係、再発防止策等の公表」を省略しても差し支えないと考えられる場合の例として挙げられている「高度な暗号化等の秘匿化が施されている場合」とは、どのような場合ですか。	例えば、電子政府推奨暗号リスト又はISO/IEC18033に掲げられている暗号アルゴリズムによって個人データを適切に暗号化し、かつ、復号(平文化)のためのかぎ(鍵)が適切に管理されている場合など、十分な秘匿性が確保されている場合は、「高度な暗号化等の秘匿化が施されている場合」に該当すると考えられます。(2007.3.30)
80	「高度な暗号化等の秘匿化として施していた措置内容を具体的に報告すること」とありますが、どのような報告の内容が考えられますか。	例えば、次のような報告の内容が考えられます。 (1)暗号化手法に関する情報として次の項目： ・用いている暗号の情報(共通鍵暗号、公開鍵暗号等の方式、AES等の暗号アルゴリズム) ・対象となる個人情報に適用していた鍵の長さ (2)暗号ソフトウェアの種類とバージョン (3)識別符号の管理等、暗号鍵の管理ポリシーとして次の項目： ・複雑さ(英字、数字、記号を、それぞれ一つ以上含む一般名詞ではない文字列、等) ・更新頻度(月に一度の変更、一定回数(復号)の度に更新、等) ・アクセス制限(個人情報管理者だけに限定、等) ・保存管理形態(ハードウェア暗号機能を持つUSBメモリにテキストファイルとして格納し個人情報管理キャビネット(あるいはストレージ)とは別の保管装置収納、市販のパスワード管理ツールを利用、等) ・その他(複数の個人情報データベース等と同じ鍵を用いない、復号実施者の記録を残す、等) (2010.4.1)



「高度な暗号化」ってなに？

当初の議論のポイント

■ 情報(の質)によるレベル分け(情報価値)が必要か？

論点#2: 情報のレベル分けの考えを導入するか IPA

- 情報の「**保有数**」でのレベル分けの考え方(案)
 - 個人情報保護ガイドラインでのレベル分けの考え方
 - 5,000
 - XXXX, XXXX (過去の月別の個人情報保有件数)

メリット

- 個人情報保護法や同ガイドラインとの相性が良い
- 区分基準が明確

デメリット

- 情報の質を考慮しない(「本人」にとっての感受と合わない)

- 情報の「**機敏度**」でのレベル分けの考え方(案)

レベル1	レベル2	レベル3	レベル4	レベル5
公開情報のみで構成	他情報と結び付くと影響が大きくなる情報	日常生活上の機敏な情報	金融情報	プライバシー情報
氏名、性別、生年月日、住所など	電話番号、メールアドレス、ユーザーIDなど	学校成績、購入履歴、行動履歴など	クレジットカード番号、保険証券番号など	従来、生体情報、居住歴など

メリット

 - 情報の質を考慮
 - 情報の質によって対策を明示的に変えられる

デメリット

 - 個人情報保護法や同ガイドラインとの相性がよくない
 - 情報の質の区分基準が個人の考えで異なる

論点#2: 情報のレベル分けの考えを導入するか IPA

- 情報の「**想定損害賠償額**」でのレベル分けの考え方(案)
 - JNSA被害金額の考え方
 - 裁判事例や漏えい事故の時の賠償金額等を参照し、各事例に当てはめて被害金額を計算
 - 想定損害賠償額 = 漏えい個人情報価値 × 情報漏えい組織の社会的責任度 × 事後対応評価

メリット

- 情報の質を一定程度考慮
- 適用対象が分かりやすい

デメリット

- 個人情報保護法や同ガイドラインとの相性がよくない
- 想定損害賠償額の算出が難しい

■ 「情報価値」によって「高度の暗号化」のレベルを変えるべきか

【現在のガイドライン上の差異】

- 暗号化: 「組織的安全管理措置」及び「技術的安全管理措置」における例示措置の一つ
- 高度な暗号化: (解読困難な暗号化を施して、本人へ被害が発生する可能性が著しく低い場合については) 情報漏えい事故発生時に「本人への通知」及び「公表」を省略しても差し支えないと考えられる対策措置

	情報価値1	情報価値2	情報価値3	情報価値4
対策レベル4	OK	OK	OK	OK
対策レベル3	OK? NG?	OK? NG?	OK? NG?	NG
対策レベル2	OK? NG?	OK? NG?	OK? NG?	NG
対策レベル1	OK? NG?	OK? NG?	OK? NG?	NG
対策不十分	OK? NG?	OK? NG?	OK? NG?	NG

やってみてわかったこと

		脅威レベル1	脅威レベル2	脅威レベル3	脅威レベル4	
想定条件	想定攻撃者の攻撃意思	【攻撃意思は弱い】 あらかじめ標的を狙うことはしない (偶発的に情報を入手)			【攻撃意思は強い】 標的を狙って攻撃を行う (意図的に情報を入手)	
	想定攻撃者の攻撃能力	【攻撃能力は低い】 対策技術を解除しようとする能力/意思はない (偶然見ること以外の行動を特に起こさない)	【攻撃能力は中度】 対策技術を解除するために、解読ツールを使わない程度で出来る攻撃(低コストの攻撃)を行う可能性あり	【攻撃能力は高い】 対策技術を解除するために、解読ツール等も活用する攻撃(高コストの攻撃)を行う可能性あり	【攻撃能力は非常に高い】 対策技術を解除するために、解読ツール等も活用した組織的攻撃(非常に高コストの攻撃)を行う可能性あり	
漏えい等態様	紛失	←→				
	誤送信	←→				
	管理ミス	←→				
	ウィルス感染	←→				→
	ハッキング			←→		
	強奪・盗難	←→				→
	内部犯行	【重大な脅威ではあるが、想定条件が他と異なるので、今回は検討対象から外す】				



一律に「高度の暗号化」を定義づけることは難しそうだ

- 脅威レベル4を考えない・・・はたして許されるか？
- データの存在位置で色々な場合分けをしてみる・・・が、想定例がありすぎ

思い切って割り切ろう・・・

事実上の脅威は「紛失・盗難だけ」に特化しよう

「なんでも使える」を目指すとは結局「何にも使えない」から

「高度な暗号化」の定義づけはあきらめよう

全部の脅威に対しての対策にはなっていないから

「暗号化がどういうことか」の定義づけはやろう

「暗号化している」ことのベースラインは示そう

暗号化しているから
大丈夫だとします (キリッ)
(認証パスワードはいいですけど)

暗号化していても
秘密鍵が見つかれば以上
解読できる可能性がある
(だから暗号化していてもダメ)

割り切った考えでのマニュアルを作りました

「暗号についての技術的な話」は極力しない

暗号の技術的なことを知らなくても日常生活で使っているから

「暗号製品を使って情報漏えい対策が正しく安全に機能するための注意点」を重点的に説明

使い方を間違えると暗号は安全に働かないから

「情報価値と対策レベルの考え方」を提示

リスクと利便性のバランスを無視した対策は形骸化するから

「代表的な製品の設定方法の手順」を図示

どこにどんな設定項目があるかすら知られていないから

「権限を有するものによる不正持ち出し」は考慮しない

「暗号化」の対策では守れないから

「解説編」と「実践編」の二部構成



解説編 ～ 知ってほしいこと～

目次	
1. はじめに	2
1.1 本書の内容及び位置付け	2
1.2 本書が対象とする読者	2
1.3 本書が対象とする範囲	3
2. 情報漏えい対策が正しく機能するために知っておくべきこと	5
2.1 端末ロックを設定するだけでは不十分 ～ 暗号化の必要性 ～	5
2.2 暗号化の仕組み	7
2.3 暗号化しさえすればそれだけで安心? ～使い方を間違えると情報漏えい対策として安全に機能しない～	9
2.3.1 暗号アルゴリズム自体の脆弱性が悪用されるケース	10
2.3.2 正規の利用者になりすまされるケース	10
2.3.3 暗号アルゴリズム以外の脆弱性が利用されるケース	10
2.4 情報漏えい対策として正しく安全に機能するために必要なこと	14
2.4.1 第三者検証された安全な暗号アルゴリズムを使う ～電子政府推奨暗号とは～	14
2.4.2 利用者を正しく見極める ～なりすまされないために注意すること～	17
2.4.2.1 正規の利用者かどうかを判断するための認証手段	17
2.4.2.2 パスワードを使った利用者認証には細心の注意を払う	18
2.4.2.3 バイオメトリクス認証で注意すべきこと	22
2.4.3 端末が信頼できる状態で暗号製品を使う	26
2.4.3.1 セキュリティパッチを適用することは必須	26
2.4.3.2 信頼できる暗号製品を使う ～セキュリティ認証制度～	26
3. 暗号化による情報漏えい対策の実施方法 ～ベースライン対策～	29
3.1 暗号化を行う方法について	29
3.2 情報価値レベルとベースライン対策の考え方について	31
3.3 端末・可搬媒体に対するベースライン対策	33
【コラム①】暗号アルゴリズム ～共通鍵暗号と公開鍵暗号～	8
【コラム②】実装攻撃ってなに?	12
【コラム③】「第三者検証された安全な暗号アルゴリズム」の重要性	15
【コラム④】DES はどのくらいのコストで解読できるか	21
【コラム⑤】指紋認証をだます方法 ～“グミ指”を知っていますか?～	24
【コラム⑥】セキュリティ認証制度とは	27
【コラム⑦】リモートワイプを導入したら	47

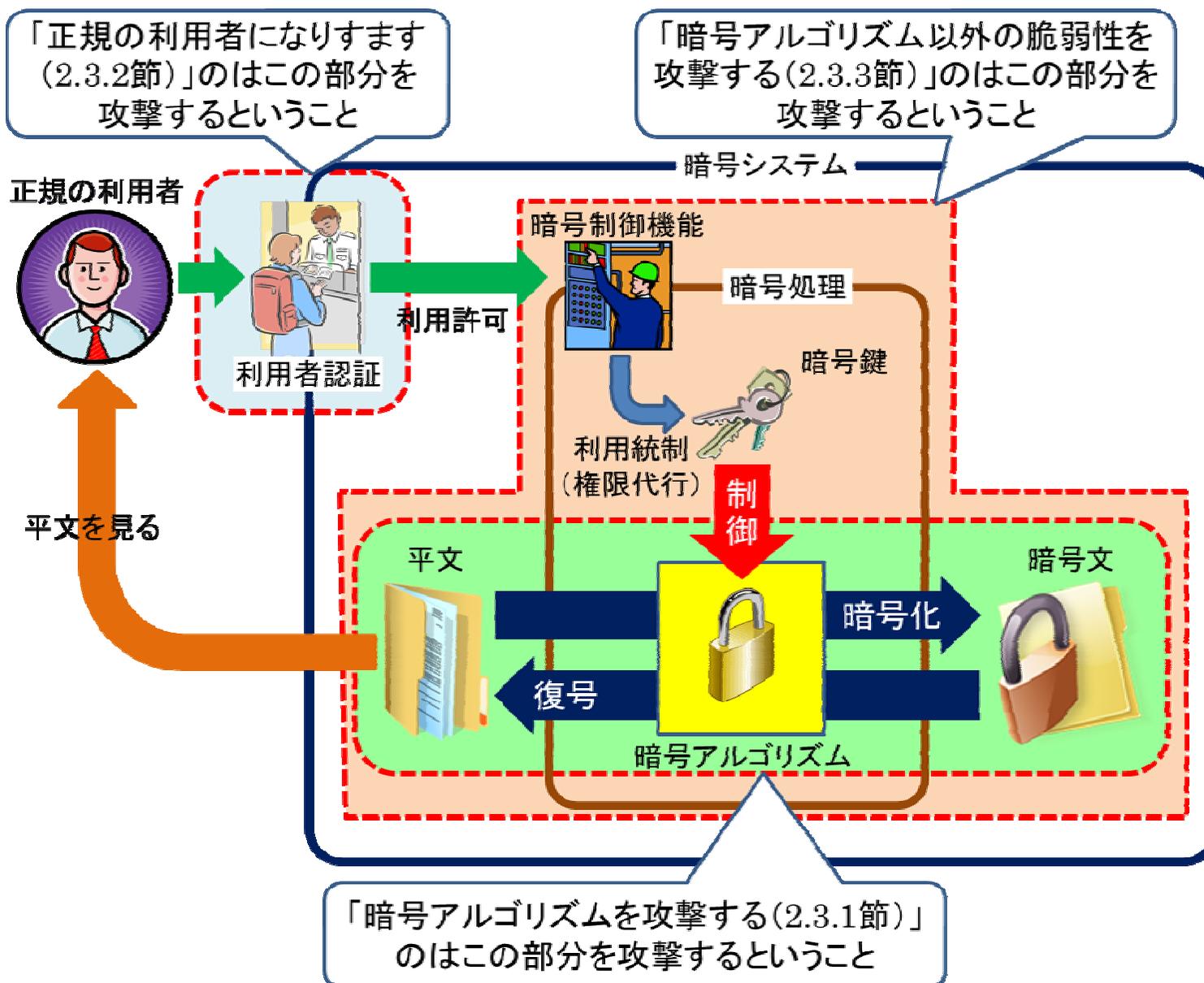
実践編 ～ どうやればよいか～

目次	
実践編 I. 情報保護対策の具体的な手法例	2
A) 端末ロックでの利用者認証による保護	3
B) ファイルの暗号化による保護	4
C) ドライブ (全記憶領域) / フォルダ (特定領域) の暗号化による保護	5
実践編 II. ユースケースと対策例	8
ユースケース 1: 情報価値レベル 1 の情報を含むファイルが保存された USB メモリを持ち運ぶ場合	8
ユースケース 2: 情報価値レベル 2 の情報が保存されたスマートフォンを持ち運ぶ場合	9
ユースケース 3: 情報価値レベル 3 の情報が保存されたノート PC を持ち運ぶ場合	12
実践編 III. 代表的な製品の具体的な設定方法の実例	14
① Windows 7, Windows 8 での設定方法一例	15
A.1 端末ロックによる利用者認証の有効化 (利用者認証の設定方法)	15
A.2 端末ロックによる利用者認証の安全性強化 (利用者認証失敗時の動作設定方法)	26
C.1 ドライブ/フォルダの暗号化設定と端末ロックによる利用者認証の有効化	32
② iOS 6 での設定方法一例	42
A.1 端末ロックによる利用者認証の有効化 (利用者認証の設定方法)	42
A.2 端末ロックによる利用者認証の安全性強化	45
C.1 ドライブ/フォルダの暗号化設定と端末ロックによる利用者認証の有効化	50
③ Android 4.x での設定方法一例	51
A.1 端末ロックによる利用者認証の有効化 (利用者認証の設定方法)	51
A.2 端末ロックによる利用者認証の安全性強化	53
C.1 ドライブ/フォルダの暗号化設定と端末ロックによる利用者認証の有効化	56
④ Microsoft Office (Word, Excel, Powerpoint) での設定方法一例	59
B.1 ファイルへの暗号化設定の有効化 (保存方法)	59
⑤ Adobe Acrobat (PDF ファイル) での設定方法一例	62
B.1 ファイルへの暗号化設定の有効化 (保存方法)	62
⑥ Imation 指紋認証付 USB メモリでの設定方法一例	66
C.3 端末起動時および端末ロックによる利用者認証の安全性強化 (バイオメトリクス認証設定、回復用パスワード (マスターパスワード) 設定)	66

攻撃者が狙うのは…どこ？

解説編

IPA



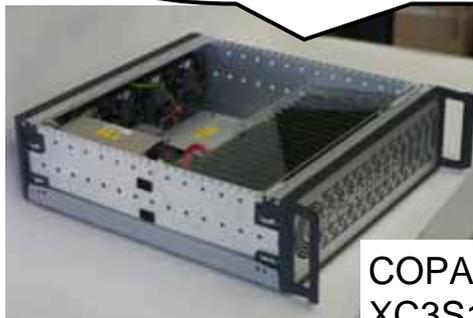
パスワードの安全性の試算例

解説編

IPA

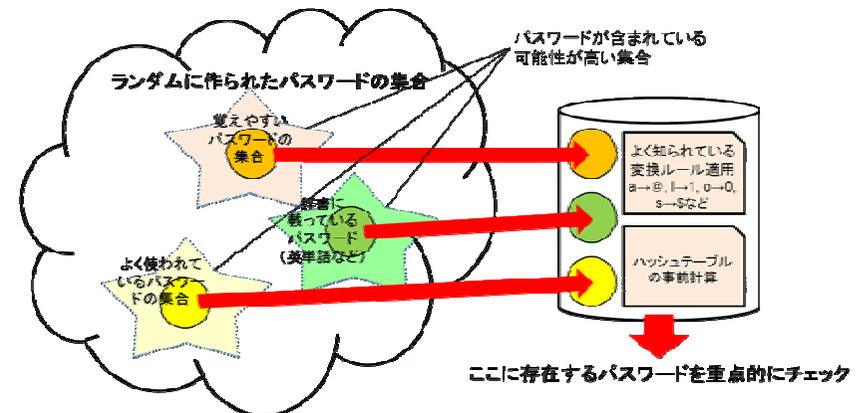
文字種類数と内訳				パスワード長			
種類数	数字	文字	シンボル	4文字	8文字	12文字	16文字
10種	0-9	なし	なし	1円未満 (計算量: $2^{13.3}$)	1円未満 (計算量: $2^{26.6}$)	約35円 (計算量: $2^{39.9}$)	約35万円 (計算量: $2^{53.2}$)
36種	0-9	a-z	なし	1円未満 (計算量: $2^{20.7}$)	約100円 (計算量: $2^{41.4}$)	約1.65億円 (計算量: $2^{62.0}$)	約276兆円 (計算量: $2^{82.7}$)
62種	0-9	A-Z a-z	なし	1円未満 (計算量: $2^{23.8}$)	約7,500円 (計算量: $2^{47.6}$)	約1,120億円 (計算量: $2^{71.5}$)	約165京円 (計算量: $2^{95.3}$)
94種	0-9	A-Z a-z	!"#\$%&'()=~ `¥{@[+*]; :}<>?_.,/	1円未満 (計算量: $2^{26.2}$)	約21万円 (計算量: $2^{52.4}$)	約16.5兆円 (計算量: $2^{78.7}$)	約129,000 京円 (計算量: $2^{104.9}$)

DES解読装置(計算量: 2^{56})
約250万円としたら...

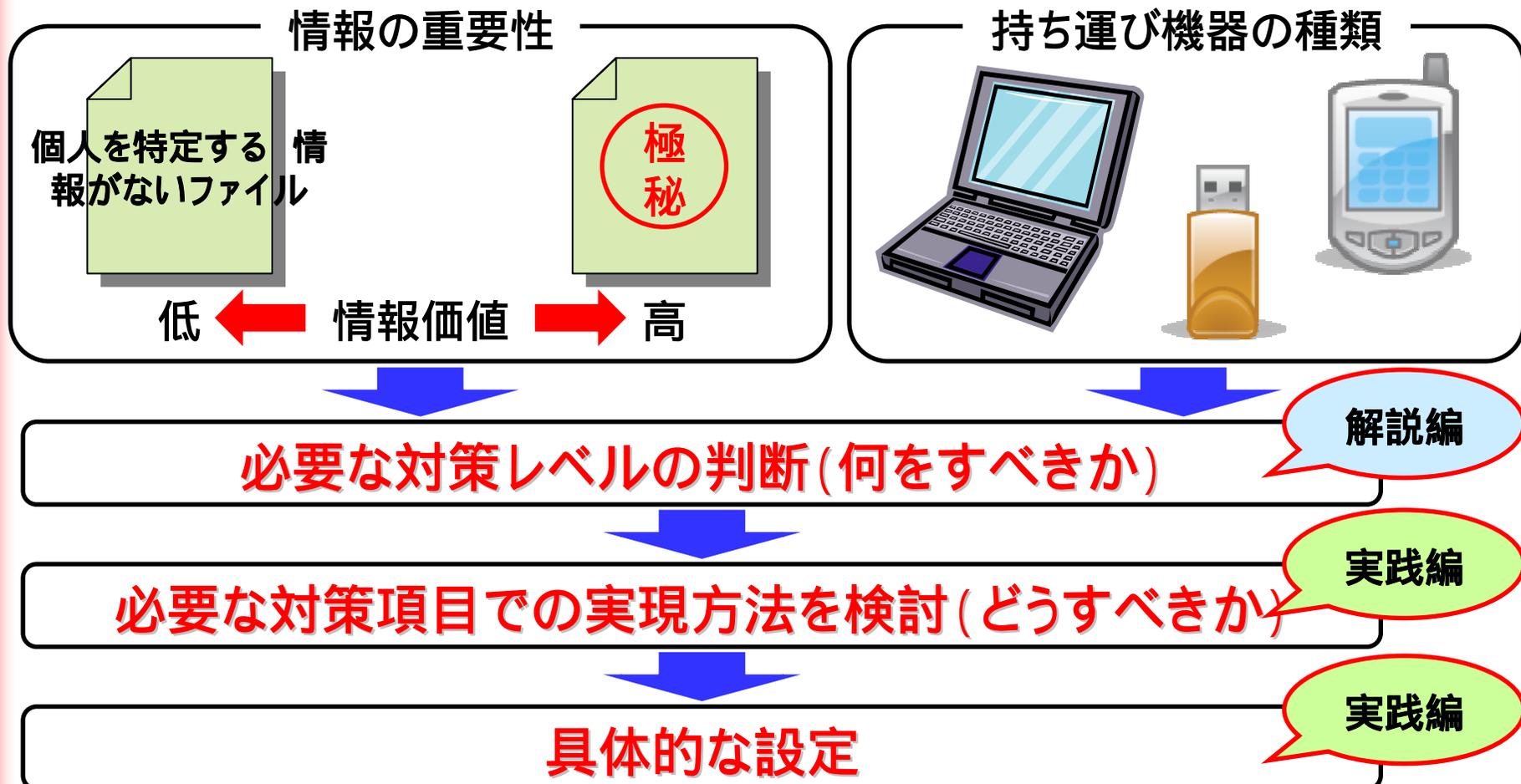


COPACOBANA S1 (Spartan-3 XC3S1000, Revision 12/2006)

実際にはもっと弱い可能性が高い...



「**守るべき情報の重要性**」と「**持ち運び機器の種類**」に応じて
暗号でどのようにデータを保護するか



本マニュアルの使い方

解説編

IPA

取り扱う情報の価値から
どの程度の対策レベルを
実現するかを判断



	情報価値レベルの考え方	対策レベルの考え方(期待効果)
レベル4	漏えいさせた場合には、 重大な悪影響をもたらす 、信用棄損のみならず、経営的にも多大な損害が発生する可能性が高い情報	暗号解読に必要な計算能力、コストが非現実的である限り、 元の情報が見られる可能性はほとんどない
レベル3	漏えいさせた場合には、 重大な悪影響をもたらす可能性 があり、信用棄損の他、場合によっては経営的にも損害が発生する可能性がある情報	対策を破るコストが情報価値を大きく上回るようにすることで、元の情報を見てもメリットがないと感じさせ、 情報を見ようと努力するモチベーションを大きく低下させる
レベル2	漏えいさせた場合でも、重大な悪影響が生じる可能性は小さいが、企業倫理上、 安易に見られることは避けたい 情報	端末・可搬媒体等を偶然入手した人がその中の 情報を見ようと努力することをあきらめさせる
レベル1	上記以外 の情報	端末・可搬媒体等を偶然入手した人が 興味本位でその中の情報を見ようとする ことをあきらめさせる

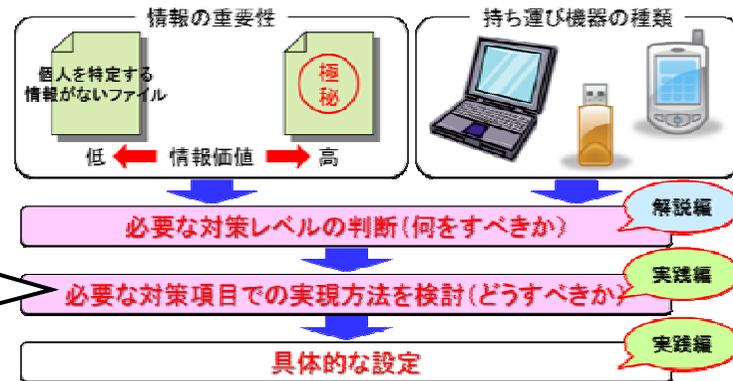
本マニュアルの使い方

解説編

実践編



具体的に実施する
ベースライン対策を選
択



解説編 必要な対策項目一覧

【対策レベル 3】

● 対策レベル 3-1:

- 例 1: 指紋認証機能付き高セキュリティノートパソコン内のドライブ暗号化の実施
- 例 2: ノートパソコン内のドライブ暗号化と利用者認証用 USB トークンの併用
- 例 3: タブレット内のドライブ暗号化とリモートワイプ設定の併用

《実施すべき項目》

- A.1 (実践編-3) 端末ロックによる利用者認証の有効化
- A.2 (実践編-3) 端末ロックによる利用者認証の安全性強化
- A.3 (実践編-3) 端末ロックによる利用者認証のさらなる安全性強化
- C.1 (実践編-5) ドライブ/フォルダの暗号化設定と端末ロックによる利用者認証の有効化
- C.2 (実践編-5) 端末起動時の利用者認証の有効化
- C.3 (実践編-5) 端末起動時および端末ロックによる利用者認証の安全性強化

【実施が望ましい項目】

- B.1 (実践編-4) ファイル暗号化の有効化
- B.2 (実践編-4) 暗号化ファイルに対するアクセス制御の強化
- B.3 (実践編-4) 暗号化ファイルに対するアクセス制御のさらなる強化
- C.4 (実践編-6) 暗号化データに対するアクセス制御の強化
- C.5 (実践編-6) 暗号鍵の管理強化

実践編 対策実現方法の一覧

<p>A) 端末ロックでの利用者認証による保護</p> <p>A.1 端末ロックによる利用者認証の有効化</p> <p>以下の設定をすべて行う。</p> <ol style="list-style-type: none"> ① 端末ロックに ② 端末ロック <p>A.2 端末ロックによ 少なくとも①の対 する。</p> <ol style="list-style-type: none"> ① 一定回数以上 な解除処理を アウト (一定 時間は、利用 ② パスワード長 ドを利用する <p>A.3 端末ロックによ 以下の方法のい 強化する。</p> <ol style="list-style-type: none"> ① パスワード強 ② 複数のパ スワード ③ トークン認 証を使用した利 用 ④ ワンタイムパ スワード ⑤ バイオメトリ ック ⑥ 認証サーバに ⑦ リモートロ ック <p>注意:</p> <ul style="list-style-type: none"> ● 複数のパ スワード ● ③でパ スワード ● トークン 	<p>C) ドライブ (全記憶領域) の暗号化設定と端末ロックによる利用者認証の有効化</p> <p>C.1 ドライブ/フォルダの暗号化設定と端末ロックによる利用者認証の有効化</p> <p>以下の設定をすべて行う。</p> <ol style="list-style-type: none"> ① 端末ロックによる利用者認証機能を有効にする (A.1と同様) ② 端末がロックされるまでの時間や条件を適切に設定する (A.1と同様) ③ ドライブ/フォルダの暗号化機能を有効にする ④ 一定回数以上端末ロックによる利用者認証に失敗した場合、端末の完全ロック (特別な解除処理をしない限り以後の利用者認証を受け付けない) もしくは一定期間ロックアウト (一定時間利用者認証を受け付けない) する。後者の場合、ロックアウトする時間は、利用環境や扱う情報価値レベルに応じて適切に設定すること (A.2と同様) ⑤ パスワード長を大きくしたり、利用する文字種を増やしたり、ビジュアルパスワードを利用するなど、パスワードの複雑度を高める (A.2と同様) <p>C.2 端末起動時の利用者認証の有効化</p> <p>以下の設定をすべて行う。</p> <ol style="list-style-type: none"> ① 端末起動時の利用者認証機能を有効にする ② 端末ロックによる利用者認証とは異なるパスワードを設定する <p>注意:</p> <ul style="list-style-type: none"> ● 端末起動時の利用者認証が複数設定される場合、共通のパスワードもしくは類似したパスワードにしないこと ● 携帯電話・スマートフォン・USBメモリ・外付けドライブストレージなどの機種によっては、端末ロックによる利用者認証 (A.1) と端末起動時の利用者認証 (C.2) が自動的に同じ設定になる場合がある。その場合には C.2 を実施しなくてよい ● BIOS設定の変更が必要となるため、必要があれば、パソコン等の知識を有する人の助言を得ること。BIOS設定に失敗すると端末自体が起動しなくなる恐れがある <p>C.3 端末起動時および端末ロックによる利用者認証の安全性強化</p> <p>以下の方法のいずれかまたは併用により、端末起動時および端末ロックによる利用者認証の安全性を強化する。</p> <ol style="list-style-type: none"> ① パスワード強度チェックに合格したパスワードを利用する。特に、すべての利用者認証がパスワードだけで認証する場合には、共通のパスワードもしくは類似したパスワードに設定しないこととし、少なくとも一つはパスワード強度チェックに合格したパスワードを利用することを強く推奨する
---	--

今回のマニュアルでも「まだまだ難しい」と言われた
暗号化の正しい利用方法を理解してもらうことはすごく大変

「暗号化」の意味・効果が関係者間できちんと定義されていないうちにいろいろな議論が進んでいないか？
「安全」の議論がかみ合わない最大の理由では？

「メジャー(基準)がない“形容詞”規定」が多くないか？
やっている対策が十分なのかどうかの判断ができない

一つのリスクだけに特化した議論をしていないか？
リスク全体を俯瞰した議論がなされない