IPA
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

はじめに

- 「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

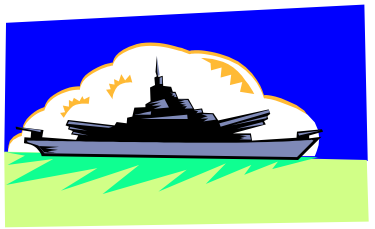
鍵をほったらかしてはダメだよね

Back to the CRYPTREC 2000

- 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、ρ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」

暗号アルゴリズムの黒船がやってきた



- 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CRYPTREC暗号リストが公表 (1)

IPA

■ 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
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS (注1)
		RSASSA-PKCS1-v1_5 (注1)
	守秘	RSA-OAEP (注1)
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号 (注2)	3-key Triple DES (注3)
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2

技術分類		名称
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
	認証付き秘匿モード	CCM
		GCM (注4)
メッセージ認証コード		CMAC
		HMAC
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3

※注釈略

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

※注釈略

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		RIPEMD-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。

体制が変わります

新しいCRYPTREC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？

「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

暗号世代交代の対策実行への難しさ

「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が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**

- 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

対処する／しないによる影響は必ずしも明確ではない

？

「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・・・

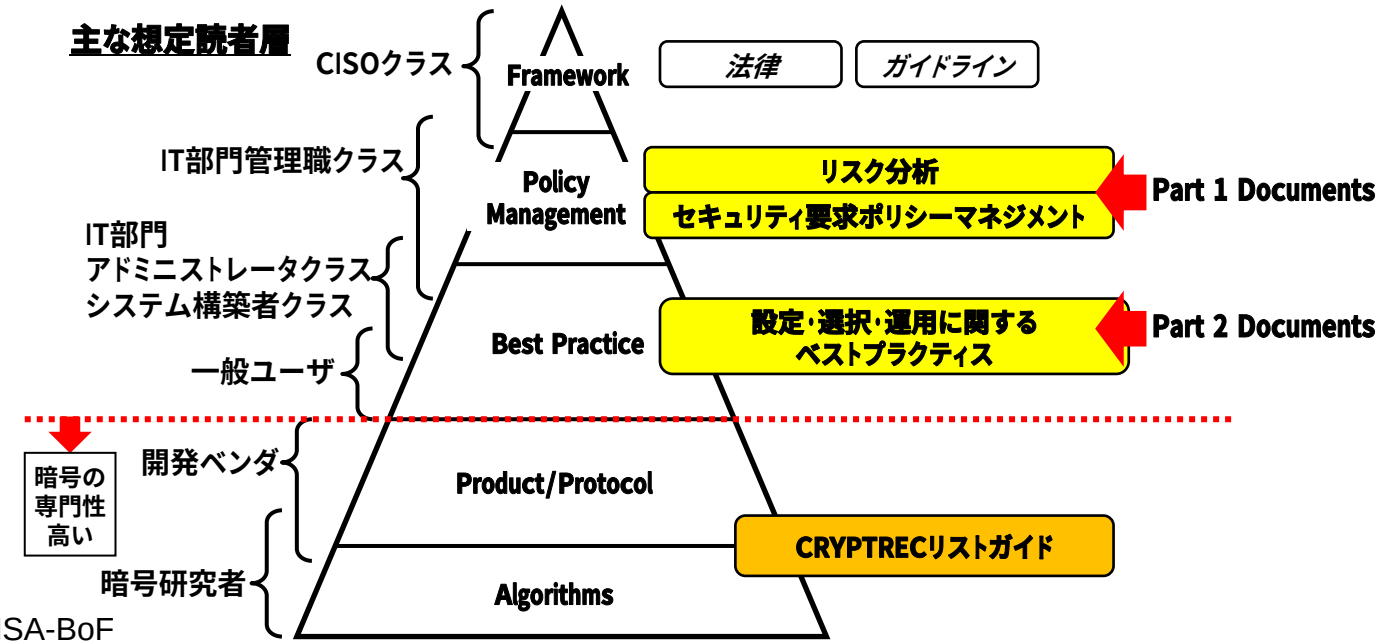
- 暗号実装に問題があるケース
  - ⇨ 実害が発生する原因としては、直接的な暗号解読よりもリスクがはるかに高い
- 運用管理上／暗号設定上の問題があるケース
  - ⇨ 暗号が正しく動くための前提条件の崩壊。利用者が管理しえない領域の問題であることも多い
- リテラシーに問題があるケース
  - ⇨ なりすましの危険性。リテラシーが低い人ほど対策を取らない可能性が高い
- モラルに問題があるケース
  - ⇨ 権限自体は正規に持っているユーザが不正行為を働く。暗号だけではまず守りきれない

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

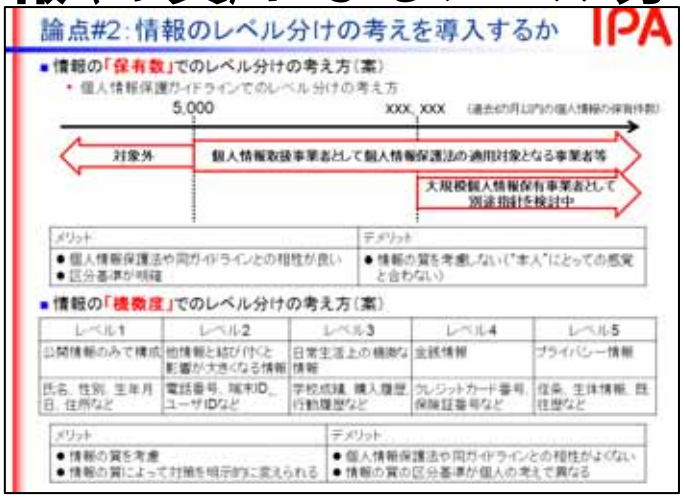
【ガイドラインFAQ】

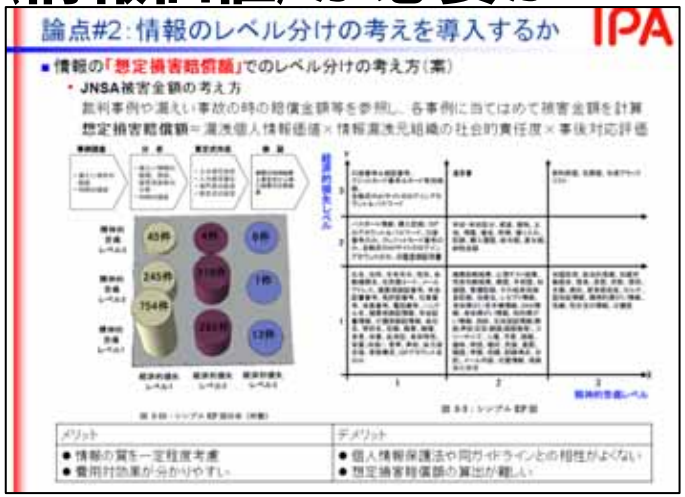
79	個人データが漏えい等したが、本人の権利利益が侵害されておらず、今後も権利利益の侵害の可能性がない又は極めて少ないと考えられるため、「影響を受ける可能性のある本人への連絡」や、「事実関係、再発防止策等の公表」を省略しても差し支えないと考えられる場合の例として挙げられている「高度な暗号化等の秘匿化が施されている場合」とは、どのような場合ですか。	例えば、電子政府推奨暗号リスト又はISO/IEC18033に掲げられている暗号アルゴリズムによって個人データを適切に暗号化し、かつ、復号（平文化）のためのかぎ（鍵）が適切に管理されていると認められる場合など、十分な秘匿性が確保されている場合は、「高度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別とバージョン (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、一定回数の復号の度に変更、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に同じ鍵を用いない、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？

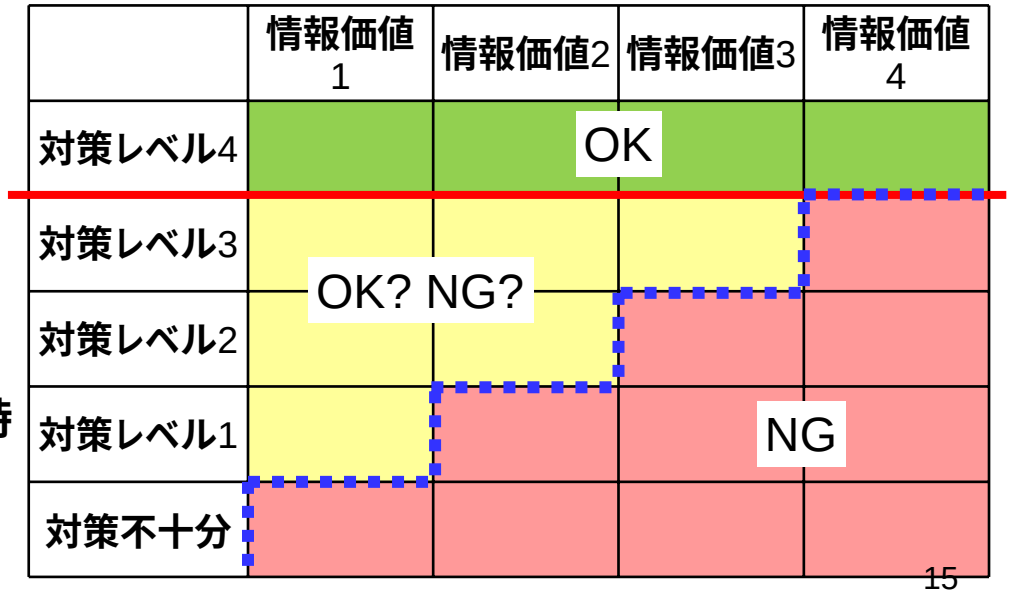




- 「情報価値」によって「高度の暗号化」のレベルを変えるべきか

【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いて、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」を省略しても差支えないと考えられる対策措置



やってみてわかったこと

IPA

		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・・・

IPA

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

~~暗号化してるから~~
~~大丈夫だと言います(キリッ)~~
~~(認証パスワード甘いですけど)~~

~~暗号化してても~~
~~秘密鍵が見つけられる以上~~
~~解読できる可能性がある~~
~~(だから暗号化してなくてもダメ)~~

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

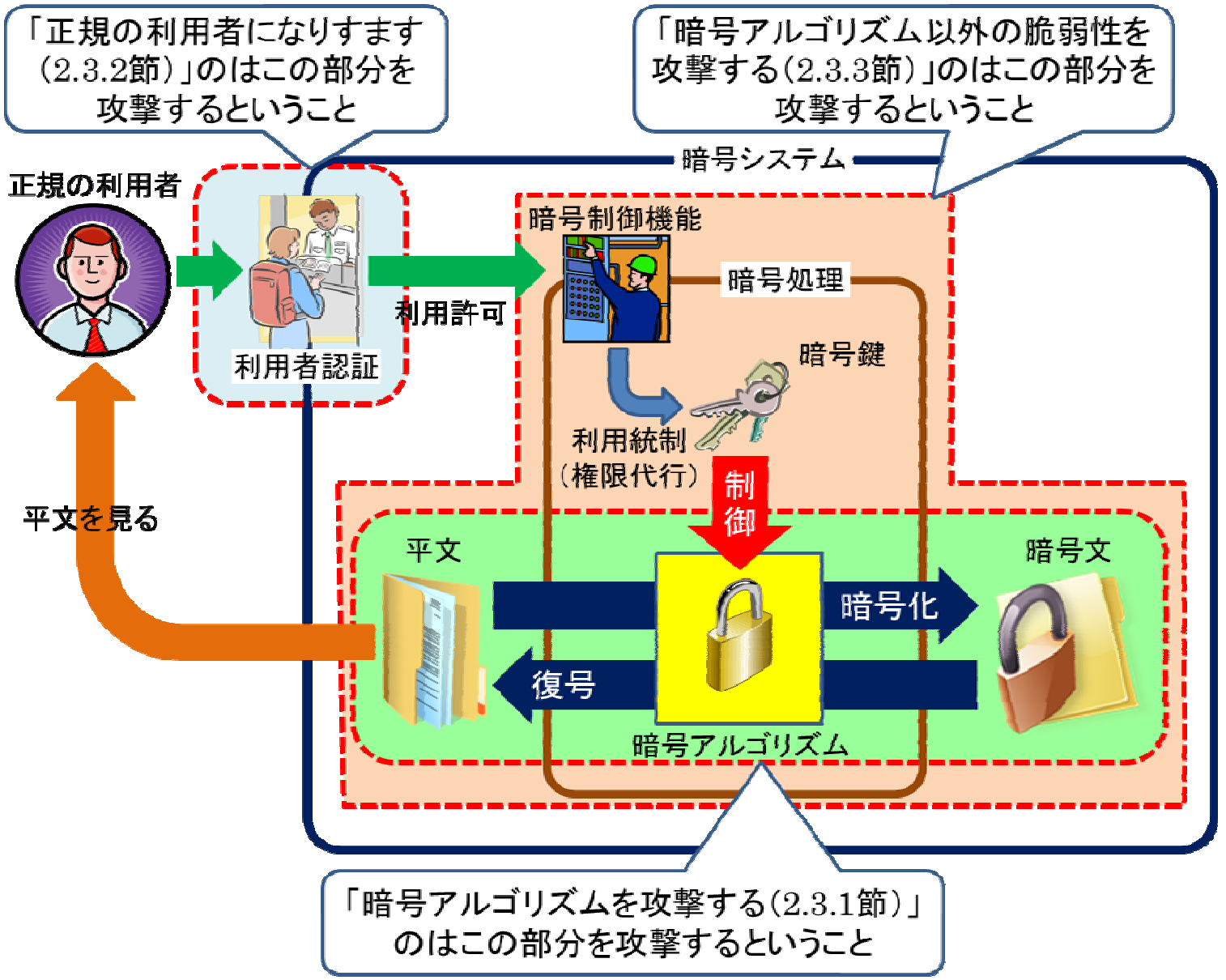
実践編 ～どうやればよいか～

目次

攻撃者が狙うのは・・・どこ？

解説編

IPA



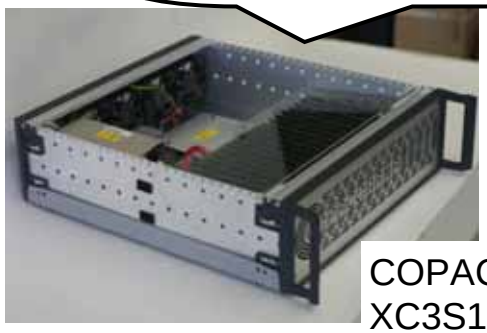
パスワードの安全性の試算例

解説編

IPA

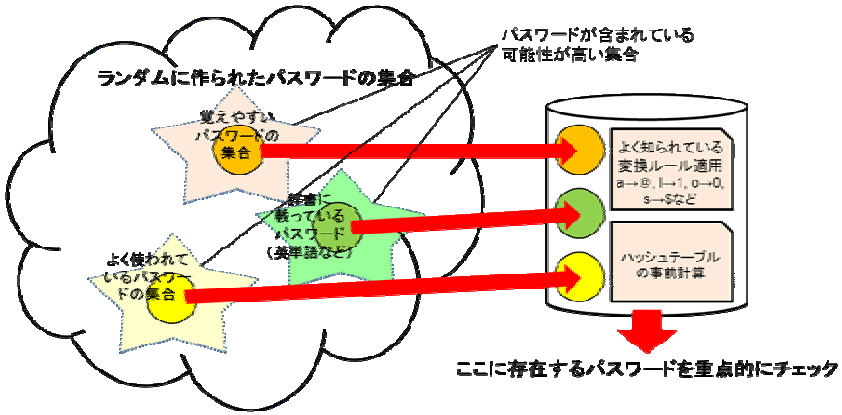
文字種類数と内訳				パスワード長			
種類数	数字	文字	ｼﾝﾎﾞﾙ	4文字	8文字	12文字	16文字
10種	0–9	なし	なし	1円未満 (計算量：$2^{13.3}$)	1円未満 (計算量：$2^{26.6}$)	約35円 (計算量：$2^{39.9}$)	約35万円 (計算量：$2^{53.2}$)
36種	0–9	a–z	なし	1円未満 (計算量：$2^{20.7}$)	約100円 (計算量：$2^{41.4}$)	約1.65億円 (計算量：$2^{62.0}$)	約276兆円 (計算量：$2^{82.7}$)
62種	0–9	A–Z a–z	なし	1円未満 (計算量：$2^{23.8}$)	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・・・



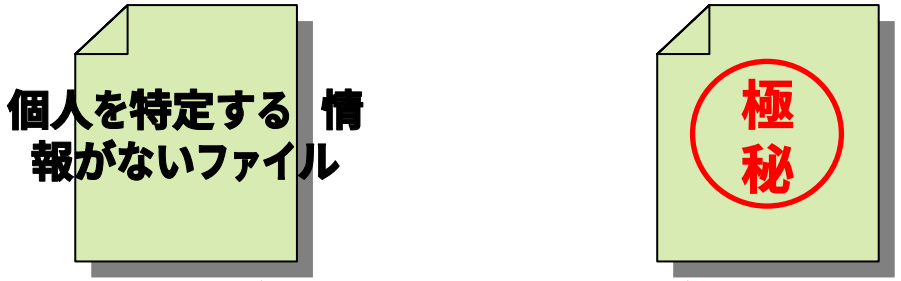
本マニュアルの使い方

解説編　実践編

IPA

「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

情報の重要性



持ち運び機器の種類

必要な対策レベルの判断（何をすべきか）　解説編

必要な対策項目での実現方法を検討（どうすべきか）　実践編

具体的な設定　実践編

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

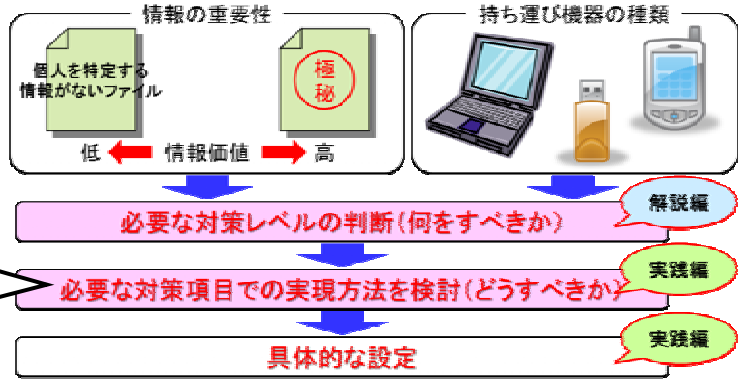
	情報価値レベルの考え方	対策レベルの考え方（期待効果）
レベル4	漏えいさせた場合には、**重大な悪影響をもたらし**、信用棄損のみならず、経営的にも多大な損害が発生する可能性が高い情報	暗号解読に必要な計算能力、コストが非現実的である限り、**元の情報が見られる可能性はほとんどない**
レベル3	漏えいさせた場合には、**重大な悪影響をもたらす可能性**があり、信用棄損の他、場合によっては経営的にも損害が発生する可能性がある情報	対策を破るコストが情報価値を大きく上回るようにすることで、元の情報を見てもメリットがないと感じさせ、**情報を見ようと努力するモチベーションを大きく低下**させる
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

IPA

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

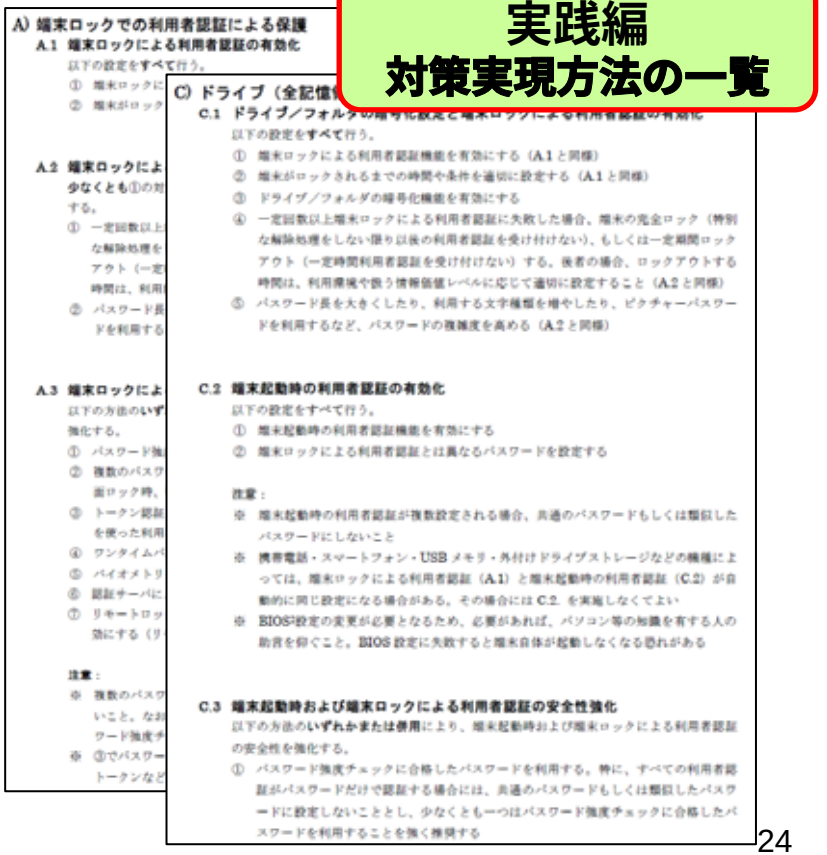
《実施すべき項目》

- 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



パネルディスカッションに向けて

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