

研究WG：副次的暗号

2011年2月7日
(WGでの意見反映、pp.11,12,30)

富士通 鮎川 一郎

副次的暗号に関する法令

1. 規制の変遷
2. WAのNote 4 (EARも同じ)
3. 副次的暗号装置 (貨物:運用通達の解釈)
4. 副次的暗号プログラム (技術:役務通達の解釈)
5. 【ご参考】Ancillary Cryptoの定義 (昔のEAR)

1. 規制の変遷

- **2008/10/3 米国でAncillary Cryptographyの概念を導入**
 - 73 FR 57495
 - Ancillary CryptographyはLE=ENCやmass market適用時、レビュー不要に
 - EAR Part 742 (Definition)でAncillary Cryptographyを定義
- **2009/12 ワッセナーリスト改正:米国の概念をワッセナーに取り込む**
 - Note 4 in Cat5-Part2 を新設し、副次的暗号は非規制に
- **2010/4/1 日本:2009年のワッセナーリストを反映**
 - 副次的暗号装置／副次的暗号プログラムの除外が新設
- **2010/6/25 米国:2009年のワッセナーリストを反映**
 - 75 FR 36481
 - EARのCCL Note 4 in Cat5-Part2を新設 → Note4で除外されるとEAR99
 - EARのPart 742のDefinitionからAncillary Cryptographyの定義削除
 - Ancillary cryptographyという用語は用いられなくなる

3

2. WAのNote 4 (EARも同じ)

Note 4 Category 5-Part 2 does not apply to items incorporating or using "cryptography" and meeting all of the following:

- a. The primary function or set of functions is not any of the following:*
 - 1. "Information security";*
 - 2. A computer, including operating systems, parts and components therefor;*
 - 3. Sending, receiving or storing information (except in support of entertainment, mass commercial broadcasts, digital rights management or medical records management); or*
 - 4. Networking (includes operation, administration, management and provisioning);*
- b. The cryptographic functionality is limited to supporting their primary function or set of functions; and*
- c. When necessary, details of the items are accessible and will be provided, upon request, to the appropriate authority in the exporter's country in order to ascertain compliance with conditions described in paragraphs a. and b. above.*

4

3. 副次的暗号装置（貨物：運用通達の解釈）

「貨物等省令第8条第九号から第十二号までの規定中の装置若しくはシステム又はその部分品」

次のいずれかに該当するものを除く。

条件1

イ 電子計算機又はその部分品若しくは**附属品**以外のものであって、次の（一）及び（二）に該当するもの（該当することが貨物の製造者、販売者又は輸出者によって書面により確認できるものに限る。）（以下「副次的暗号装置」という。）

（一）当該貨物の有する**主たる機能**が次のいずれにも該当しないもの

- 1 情報システムのセキュリティ管理
- 2 情報の送信、受信又は記録及び保存（娯楽施設又は装置の有する機能であるもの、商業放送、デジタル著作権管理又は医療用の記録管理のために行われるものを除く。）
- 3 有線若しくは無線回線網による電気通信回線の構築、管理又は運用

（二）当該貨物の有する暗号機能が当該貨物の**主たる機能の支援のためにのみ**用いられているもの

ロ（省略）

条件2

5

4. 副次的暗号プログラム（技術：役務通達の解釈）

「貨物等省令第21条第1項第七号、第八号の二及び第九号の規定中のプログラム」

電子計算機を使用するために設計したプログラム以外のプログラムであって、次のイ及びロに該当するものを除く。（該当することが技術の供給者、販売者又は提供者によって書面により確認できるものに限る。）

条件1

イ 当該プログラムの有する**主たる機能**が次のいずれにも該当しないもの

- （一）情報システムのセキュリティ管理
- （二）情報の送信、受信又は記録及び保存（娯楽施設又は装置の有する機能であるもの、商業放送、デジタル著作権管理又は医療用の記録管理のために行われるものを除く。）
- （三）有線若しくは無線回線網による電気通信回線の構築、管理又は運用

ロ 当該プログラムの有する暗号機能が**主たる機能の支援のためにのみ**用いられているもの

条件2

6

5. 【ご参考】Ancillary Cryptoの定義(昔のEAR)

Part 742 (Definition) April 20, 2010 (2010/6/25直前のEAR、現在は削除済み)
"Ancillary cryptography".

The incorporation or application of "cryptography" by items that are not primarily useful for computing (including the operation of "digital computers"), communications, networking (includes operation, administration, management and provisioning) or "information security".

N.B. Examples of commodities and software that perform "ancillary cryptography" are items specially designed and limited to:

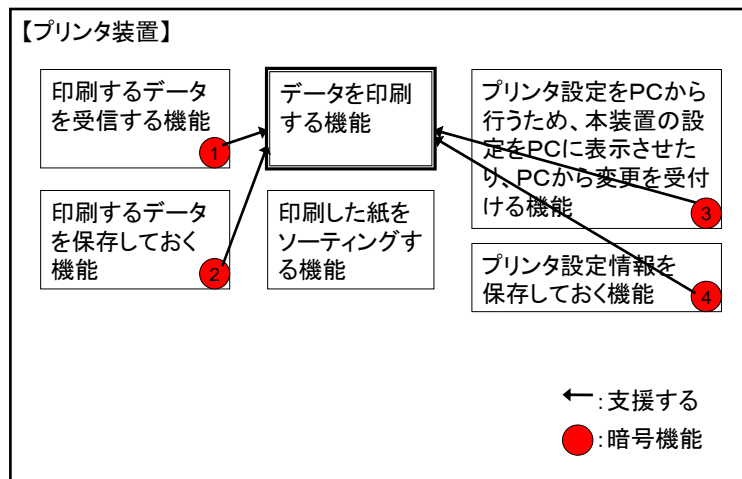
Piracy and theft prevention for software, music, etc.; games and gaming; household utilities and appliances; printing, reproduction, imaging and video recording or playback (but not videoconferencing); business process modeling and automation (e.g., supply chain management, inventory, scheduling and delivery); industrial, manufacturing or mechanical systems (including robotics, other factory or heavy equipment, and facilities systems controllers, such as fire alarms and HVAC); automotive, aviation and other transportation systems¹. Commodities and software included in this description are not limited to wireless communication and are not limited by range or key length.

¹ For the purpose of this definition, the term "transportation systems" does not include any Automatic Identification System (AIS) / Vessel Traffic Service (VTS). Secure AIS/VTS and their maritime applications are not considered "ancillary cryptography".

副次的暗号の判断の流れ

1. 「主たる機能」は何か？
2. 「条件1」の確認
= 「**主たる機能**」が「条件1」を満足することの確認
3. 「条件2」の確認
= 「**暗号機能**」が「主たる機能」の支援のためにのみ用いられていることの確認

ケーススタディ



9

ケーススタディ

1. 「主たる機能」=「データを印刷する機能」
2. 「データを印刷する機能」が「条件1」OK
3. 4箇所にある暗号機能は、「データを印刷する機能」を司っている訳ではないが、「データを印刷する機能」を支援している。またその支援以外の目的には使用していない。

→ となれば、副次的暗号装置になる。

10

整理を要する点

1. 主たる機能
2. 条件1
3. 条件2
4. 複合製品
5. 電子計算機を使用するために設計したプログラム
6. Webブラウザ関連
7. 部分品

11

1. 主たる機能

「主たる機能」の解釈

◎ 貨物/プログラムにおいて、
その第一の目的/用途を実現するための機能
目安：商品名／商品カテゴリ



その機能なしでは、
そもそもその商品名で呼ぶことができないような機能
≡ 「主たる機能」

12

1. 主たる機能

主たる機能は何か？

→これを考えるとき、

個々の暗号機能のことは忘れて、
この装置は何装置か?という視点が大切

Q:暗号を「情報の保存」に使用しているから、「条件1」が満足できないのだけど・・・？

A:「条件1」を確認する対象は、個々の暗号ではなく「主たる機能」です。

13

1. 主たる機能(ケーススタディ)

主たる機能は何か？

「主たる機能」=「データを印刷する機能」

(注)装置の主たる機能をひとつ決める。

但し、複合装置の場合は、あとで説明する。

⇒「主たる機能」が決まると、次の「条件1」を満足するか？
の確認に移ります。

14

2. 条件1(電子計算機の附属品)

- ワッセナーアレンジメントでの表現
 - Category 4 : related equipment
 - Category 5 - Part 1 : accessories
 - Category 5 – Part 2(Note4:副次的暗号) : parts
- 日本法令での表現
 - 8の項 : 附属装置
 - 9の項(通信) : 附属品
 - 9の項(情セの副次的暗号解釈) : 附属品

↳ 部品のようなもの

15

2. 条件1(電子計算機の附属品)

電子計算機



プリンタ装置

スキャナー装置

ハードディスク装置

デジタルメモリー装置

冷蔵庫

ステレオ装置

音楽用デジタルメモリー
プレーヤー

8の項でいう
電子計算機
の附属装置

8の項でいう
電子計算機
の附属装置でない

副次的暗号でいう
電子計算機の
附属品ではない

「コンピュータガイドンス 2010」のp100を参照

16

2. 条件1(電子計算機の附属品)

【電子計算機関連】

概念的には

- 「電算処理をする装置」と「記録・保存する装置」は副次的暗号装置になり得ないが、
- その他周辺装置は「条件1」を満たしうる。(副次的暗号装置の候補になりうる。)

17

2. 条件1(ケーススタディ)

A) プリンタ装置は電子計算機又はその部分品若しくは附属品か？

「主たる機能」は、

《「暗号機能」は、…》ではない。

C)の機能を持つ暗号を用いているが、条件1の判断には関係ない。

B) 情報システムのセキュリティ管理か？

C) 情報の送信、受信又は記録及び保存か？

D) 有線若しくは無線回線網による電気通信回線の構築、管理又は運用か？

→ **AからDの全てに、「No」なので「条件1」を満足**

18

2. 条件1(情報システムのセキュリティ管理)

- ワッセナーアレンジメントでの表現
 - Category 5 – Part 2(Note4:副次的暗号) :
Information security
- 日本法令での表現
 - 9の項(情セの副次的暗号解釈) :
情報システムのセキュリティ管理

主たる機能が、Category5 Part2のものは、副次的暗号になり得ない。

例: 暗号用IC、暗号ライブラリ、暗号プログラム開発ツール

19

2. 条件1(監視制御関連)

- 「有線若しくは無線回線網による電気通信回線の構築、管理又は運用」は、イメージ的には、「**通信インフラシステムを監視制御する装置**」が副次的暗号になり得ないことを表現している。
- 「監視制御される装置」は、「監視制御する装置」と通信するための暗号機能を実装する場合がある。これは通信インフラの場合に限らない。「監視制御される装置」は、何らかの主たる機能があり、その主たる機能が正常動作するように設定を受けたり、主たる機能の動作が正常か異常かを報告する目的で、「監視制御する装置」と暗号通信を行なっている。従って、「**監視制御される装置**」の主たる機能は、通常「**有線若しくは無線回線網による電気通信回線の構築、管理又は運用**」ではなく、他の条項で判断されることになる。

20

3. 条件2

装置内の暗号機能を洗い出し、

- 全ての暗号機能が、「主たる機能」の支援のためにのみ用いられている

⇒ 条件2を満足する

- ある暗号機能が、「主たる機能」以外のために用いられている場合

⇒ 条件2を満足しない

21

3. 条件2(ケーススタディ)

- **暗号1:「印刷するデータを受信する機能」部の暗号**

「データを印刷する」目的で、データを受信する時のためだけの暗号=OK

- **暗号2:「印刷するデータを保存しておく機能」部の暗号**

「データを印刷する」目的で、前段階としてデータを保存しておくためだけの暗号=OK

- **暗号3:「プリンタ設定をPCから行うため、本装置の設定をPCに表示させたり、PCから変更を受付ける機能」部の暗号**

「データを印刷する」のに装置設定は必須で、その設定のための通信用にだけ使用される暗号=OK

- **暗号4:「プリンタ設定情報を保存しておく機能」部の暗号**

「データを印刷する」のに装置設定は必須で、その設定情報保存用にだけ使用される暗号=OK

⇒ 上記全てを確認できたら、条件2を満足 ⇒ 副次的暗号装置

22

3. 条件2(事例1, 2)

【事例1】

当該装置の主たる機能処理中のみ、データを暗号化して保存するケース。

→「主たる機能の支援のためにのみ」の要件を満たす。

【事例2】

当該装置にパソコンを接続して、パソコンのブラウザや当該装置専用のソフトを用いて、(初期)設定をしたり現状の設定値を表示したりする場合で、当該装置とパソコン間の通信路を暗号化するためだけに、当該装置に暗号機能を実装したケース。

→当該装置の主たる機能を正常に動作させるために、設定したり、現状の設定を表示するのであるから、そのための通信路にだけに暗号を用いるのであるならば、「主たる機能の支援のためにのみ」の要件を満たす。

23

3. 条件2(事例3, 4)

【事例3】

当該装置が、装置故障等をモニタしている集中監視機器と通信する場合に、その通信路を暗号化するケースがある。通信内容としては、故障した日時、故障の程度、故障箇所など。

→当該装置の主たる機能の正常動作を保證するために集中監視装置と情報のやりとりをしているのであるから、そのための通信路にだけに暗号を用いるのであるならば、「主たる機能の支援のためにのみ」の要件を満たす。

【事例4】

- ・本体装置と補助装置(リモコンなど)間を暗号通信するケース
- ・1台でもある機能が動作するが、複数台でもそれと同一機能を実現できるようなもので、その複数装置間で暗号通信をするケース

→暗号がその通信路のためだけに使用されるならば、「主たる機能の支援のためにのみ」の要件を満たす。

24

4. 複合装置

以下のとおり用語を使い分ける。

単一製品

(該非判定対象)

装置

機能A

機能B

機能C

<単一製品の例>

・ルータ装置

複合製品

(該非判定対象)

装置1

機能A

機能B

機能C

装置2

機能P

機能Q

機能R

装置3

機能X

機能Y

機能Z

<複合製品の例>

・MPF(マルチファンクションプリンタ)装置

装置1=プリンタ装置

装置2=スキャナ装置

装置3=コピー装置

・携帯電話装置

装置1=音声・データ通信装置

装置2=金融決済用ICカード装置

装置3=カメラ装置

25

4. 複合製品

- 通常、装置の主たる機能はひとつ選ぶ。

- 複合装置の場合は装置ごとに**

- 8条9イの除外(認証のみ等)
- へから力の除外
- 副次的暗号

による除外が適用可能か否かを判断する。

- 複合装置の最終判定

- **全ての装置が規制除外される場合:**
→ **複合装置は規制除外される。**
- いずれかの装置が規制除外できない場合:
→ 複合装置は規制除外されず、暗号特例適用可否の検討へ。

複合装置の中で、
どの装置が
「主たる装置」か
を決めるのでは
ない。

26

5. 電子計算機を使用するために設計したプログラム

- 貨物等省令第20条第1項第七号
第7条に該当するものを使用するために設計したプログラム又は～
- 役務通達の解釈の8の項
「貨物等省令第20条第1項第七号中の設計したプログラム」
→アプリケーションプログラム(応用プログラム)であって、貨物等省令第7条に該当する電子計算機で実行するためにはオペレーティングシステムを必要とするものを含まない。

27

5. 電子計算機を使用するために設計したプログラム

- 副次的暗号プログラムの定義にある
「電子計算機を使用するために設計したプログラム以外のプログラムであって、次のイ及びロに該当するものを除く。」
の「使用するために設計したプログラム」においても、同様に「アプリケーションプログラム(応用プログラム)であって、貨物等省令第7条に該当する電子計算機で実行するためにはオペレーティングシステムを必要とするものを含まない。」と考える。

→OS上で動作するアプリケーションプログラムは、副次的暗号の候補となりうるので、プログラム自体がもつ機能の中から主たる機能を決めて、条件1と条件2の確認をする。

28

6. Webブラウザ関連

- **インターネットエクスプローラー等のブラウザそのものは**、不特定のサーバーと通信して表示・設定することを「主たる機能」としているプログラムなので、「主たる機能」が「情報の送信・受信」にあたり**副次的暗号にはならない**。
- **このブラウザ機能をそのまま実装した貨物やプログラムは多くの場合**、それらの持つ「主たる機能」の支援以上のことができる(任意のサーバーと通信できる)ことになり、「条件2」を満足できず**副次的暗号にはならない**。但し、「主たる機能」関連のサーバーにしかアクセスできないような仕組みが施されたものであれば副次的暗号になりうる。
- 上記はブラウザの議論であって、Webインタフェースが全て副次的暗号になり得ないのではない。装置やプログラムの初期設定などを、PCのブラウザから行ってもらうために、**Webサーバー機能を持った装置やプログラムは、副次的暗号装置や副次的暗号プログラムになりうる**。
- **Eメールのメーラそのものは**、「主たる機能」が「情報の送信・受信」にあたり**副次的暗号にはならない**。

29

7. 部分品

- 副次的暗号装置(非該当)の部分品の考え方
 - 副次的暗号装置(非該当)の専用部分品
 - ⇒ **副次的暗号装置の除外が適用可能(非該当)**
 - 汎用の部分品
 - ⇒ **部分品単体で判断**
- 副次的暗号プログラム(非該当)について
 - 副次的暗号プログラム(非該当)の専用プログラム
 - ⇒ **副次的暗号プログラムの除外が適用可能(非該当)**
 - 汎用のプログラム部品
 - ⇒ **プログラム部品単体で判断**

**専用か？ 汎用か？
の見極めが大切**

30

事例

1. 通信・情報セキュリティガイダンス 2010. 9版 pp.69, 250
2. 米国BISのホームページ Encryption FAQs
 - No.15 : What is Note 4? http://www.bis.doc.gov/encryption/enc_faqs.htm#15
3. 米国Federal Register
 - 06/25/10 75 FR 36481
 - Encryption Export Controls: Revision of License Exception ENC and Mass Market Eligibility, Submission Procedures, Reporting Requirements, License Application Requirements, and Addition of Note 4 to Category 5, Part 2
4. 【ご参考】Ancillary Cryptography
 - 10/03/08 73 FR 57495 Encryption Simplification
 - Part 742 (Definition) April 20, 2010 (2010/6/25直前のEAR、現在は削除済み)
5. その他の事例

31

1. ガイダンスの事例

| ページ | 条件1を満足する事例 | 条件1を満足しない事例 |
|---------------|---|--|
| p.69 p.250 | <ul style="list-style-type: none"> • 民生用自動車 • 家電品 • ゲーム機 • テレビ受信装置 • 複写機 • プリンター(印刷機) • スキャナー • 医療機器 • 娯楽施設、娯楽設備、娯楽装置(映画/遊具等) • 商業放送 • デジタル著作権管理 • 医療用の記録管理 • オーディオ・ビデオ機器 • 著作権/複製管理ツール • 業務プロセス改善/自動化(BPM/BPA)ツール • 空調設備 • 産業用/工場用機械システム (産業ロボット/生産ラインの装置等) • 自動車/航空機/交通システム | <ul style="list-style-type: none"> • 汎用的な電子計算機であるサーバ • 汎用的な電子計算機であるパソコン • 情報セキュリティ製品 (ネットワークの不正アクセス防止、 データ不正持ち出し防止等) • VPN装置 • ルーター • ネットワークスイッチ • 無線LAN • 携帯電話 • ストレージ • HDD • 電気通信回線管理・運用装置 |

32

2. BIS Homepageの事例(1/2)

| 大分類 | 事 例 |
|---|--|
| Consumer applications | <ul style="list-style-type: none"> • piracy and theft prevention for software or music; • music, movies, tunes/music, digital photos – players, recorders and organizers • games/gaming – devices, runtime software, HDMI and other component interfaces, development tools • LCD TV, Blu-ray / DVD, video on demand (VoD), cinema, digital video recorders (DVRs) / personal video recorders (PVRs) – devices, on-line media guides, commercial content integrity and protection, HDMI and other component interfaces (not videoconferencing); • printers, copiers, scanners, digital cameras, Internet cameras – including parts and sub-assemblies • household utilities and appliances |
| Business / systems applications: systems operations, integration and control | <ul style="list-style-type: none"> • business process automation (BPA) – process planning and scheduling, supply chain management, inventory and delivery • transportation – safety and maintenance, systems monitoring and on-board controllers (including aviation, railway, and commercial automotive systems), 'smart highway' technologies, public transit operations and fare collection, etc. • industrial, manufacturing or mechanical systems - including robotics, plant safety, utilities, factory and other heavy equipment, facilities systems controllers such as fire alarms and HVAC • medical / clinical – including diagnostic applications, patient scheduling, and medical data records confidentiality • academic instruction and testing / on-line training - tools and software • applied geosciences – mining / drilling, atmospheric sampling / weather monitoring, mapping / surveying, dams / hydrology |

33

2. BIS Homepageの事例(2/2)

| 大分類 | 事 例 |
|---|---|
| Research / scientific / analytical | <ul style="list-style-type: none"> • business process management (BPM) – business process abstraction and modeling • scientific visualization / simulation / co-simulation (excluding such tools for computing, networking, cryptanalysis, etc.) • data synthesis tools for social, economic, and political sciences (e.g., economic, population, global climate change, public opinion polling, etc. forecasting and modeling) |
| Secure intellectual property (IP) delivery and installation | <ul style="list-style-type: none"> • software download auto-installers and updaters • license key product protection and similar purchase validation • software and hardware design IP protection • computer aided design (CAD) software and other drafting tools |

34

3. 2010/6/25のFRの事例

| FR | 事例 |
|--|--|
| 06/25/10 75 FR 36481 pp. 36487- 36488 | <ul style="list-style-type: none"> • Piracy and theft prevention for software or music; • games and gaming; • household utilities and appliances; • printing, reproduction, imaging and video recording or playback (not videoconferencing); • business process modeling and automation (e.g., <i>supply chain</i> management, inventory, scheduling and delivery); • industrial, manufacturing or mechanical systems (e.g., <i>robotics</i>, heavy equipment, facilities systems such as fire alarm, HVAC); • Automotive, aviation, and other transportation systems; • LCD TV, Blu-ray/DVD, video on demand (VoD), cinema, digital video recorders (DVRs)/ personal video recorders (PVRs); • on-line media guides, commercial content integrity and protection, HDMI and other component interfaces; • medical/clinical—including diagnostic applications, patient scheduling, and medical data records confidentiality; • academic instruction and testing/on-line training—tools and software; • applied geosciences—mining/drilling, atmospheric sampling/weather monitoring, mapping/surveying, dams/hydrology; • scientific visualization/simulation/co-simulation (excluding such tools for computing, networking, or cryptanalysis); • data synthesis tools for social, economic, and political sciences (e.g., <i>economic, population</i>, global climate change, public opinion polling, forecasting and modeling); • software and hardware design IP protection; • computer aided design (CAD) software and other drafting tools |

35

4. 【ご参考】 Ancillary Cryptoの事例

| 旧Part 772 | 事例 |
|--|--|
| Part 742 (Definition) April 20, 2010 (2010/6/25直前のEAR、現在は削除済み) | <ul style="list-style-type: none"> • piracy and theft prevention for software, music, etc.; • games and gaming; • household utilities and appliances; • printing, reproduction, imaging and video recording or playback (but not videoconferencing); • business process modeling and automation (e.g., <i>supply chain</i> management, inventory, scheduling and delivery); • industrial, manufacturing or mechanical systems (including robotics, other factory or heavy equipment, and facilities systems controllers, such as fire alarms and HVAC); • automotive, aviation and other transportation systems¹ <p><u>¹ For the purpose of this definition, the term 'transportation systems' does not include any Automatic Identification System (AIS) / Vessel Traffic Service (VTS). Secure AIS/VTS and their maritime applications are not considered "ancillary cryptography".</u></p> |

36

5. その他の事例

| 大分類 | 条件1を満足する事例 | 条件1を満足しない事例 |
|-----|---|---|
| ハード | <ul style="list-style-type: none"> パソコン・サーバーのディスプレイ装置だけ 無停電電源装置(サーバー等に使用) 商業放送の送信装置 商業放送の受信装置 計算機システムを監視制御する装置 装置の診断治具 | <ul style="list-style-type: none"> 暗号用IC CPU、CPUの周辺LSI ストレージの制御専用LSI 無線LAN用IC 携帯電話システムの基地局 基幹インフラの光伝送装置、無線伝送装置 通信インフラネットワークを監視制御する装置 |
| ソフト | <ul style="list-style-type: none"> OS上で動作するアプリケーションプログラムで、条文的(一)から(三)に当たらないもの。 (例) 特定ユーザ向けの業務アプリ (営業用、人事用、経理用のアプリなど) 副次的暗号装置となったプリンタ装置やスキャナ装置のその装置専用の機能実現ファームウェア 副次的暗号装置となった商用放送関連装置のその装置専用の機能実現ファームウェア 計算機システムを監視制御するプログラム 装置の診断プログラム | <ul style="list-style-type: none"> OS、BIOS 暗号ライブラリ 暗号プログラム開発ツール ブラウザ(情報の送受信をして表示するのが主機能) データの記録・保存が主機能のアプリケーションプログラム ストレージ装置の情報記録・保存の機能を司るファームウェア 副次的暗号装置にならない通信装置の送信・受信機能を司るファームウェア 通信インフラネットワークを監視制御するプログラム |

37

公開されている解説

BIS Update2010の暗号ワークショップにおけるQ&A

-- <http://bisecp.videohostpro.com/transcripts%5C15.pdf>

-- <http://bisecp.videohostpro.com/transcripts%5C16.pdf>

38