参考資料3 ： FIPSテスト結果

FIPS PUB 140-1

①試験暗号データ量　10Mbyte

②ランダム抽出したnビット番目から固定長「20000bit」の範囲でのデータ分布に関する試験

FIPS PUB 140-1 test #1

//1-20,000bit

The monobit test	X=	9,916	pass	(pass if 9,654 <X <10,346)
The poker test	X=	26.304	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2,436	2,477	pass	(pass if 2,267 <X <2,733)
2	1,263	1,250	pass	(pass if 1,079 <X <1,421)
3	655	659	pass	(pass if 502 <X <748)
4	315	315	pass	(pass if 223 <X <402)
5	154	124	pass	(pass if 90 <X <223)
6+	159	156	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

FIPS PUB 140-1 test #2

//20,000,001-20,020,000bit

The monobit test	X=	10,053	pass	(pass if 9,654 <X <10,346)
The poker test	X=	6.2016	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2,467	2,469	pass	(pass if 2,267 <X <2,733)
2	1,248	1,251	pass	(pass if 1,079 <X <1,421)
3	659	641	pass	(pass if 502 <X <748)
4	329	317	pass	(pass if 223 <X <402)
5	155	162	pass	(pass if 90 <X <223)
6+	131	150	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

FIPS PUB 140-1 test #3

//40,000,001-40,020,000bit

The monobit test	X=	10,118	pass	(pass if 9,654 <X <10,346)
The poker test	X=	9.7984	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2,531	2,487	pass	(pass if 2,267 <X <2,733)
2	1,268	1,253	pass	(pass if 1,079 <X <1,421)
3	613	614	pass	(pass if 502 <X <748)
4	320	348	pass	(pass if 223 <X <402)
5	155	153	pass	(pass if 90 <X <223)
6+	134	165	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

FIPS PUB 140-1 test #4

//60,000,001-60,020,000bit

The monobit test	X=	10,079	pass	(pass if 9,654 <X <10,346)
The poker test	X=	9.2032	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2,495	2,536	pass	(pass if 2,267 <X <2,733)
2	1,300	1,243	pass	(pass if 1,079 <X <1,421)
3	636	608	pass	(pass if 502 <X <748)
4	306	309	pass	(pass if 223 <X <402)
5	157	164	pass	(pass if 90 <X <223)
6+	130	164	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

FIPS PUB 140-1 test #5

//79,980,001-80,000,000bit

The monobit test	X=	9,968	pass	(pass if 9,654 <X <10,346)
The poker test	X=	13.9648	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2,577	2,520	pass	(pass if 2,267 <X <2,733)
2	1,225	1,306	pass	(pass if 1,079 <X <1,421)
3	604	618	pass	(pass if 502 <X <748)
4	323	306	pass	(pass if 223 <X <402)
5	144	144	pass	(pass if 90 <X <223)
6+	171	150	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

Confidence
Clever
Chaos
Crypto System

Focus Systems
Bring Computer Solutions into Focus

C4Fingered

C4-Fingeredは、指紋認証とC4暗号を組合わせたセキュリティツールです。USB指紋認証製品で、持ち運びも簡単。PC利用者の本人認証およびデータの暗号化により、第三者によるPCの不正利用や盗難等による情報漏洩を防ぎ、大切な情報を守ります。

Concept

●指紋認証

パスワードやICカードによる認証は、忘却や盗難・紛失による第三者のPC不正利用の危険性があります。そこで、世界中でただ一人本人のみが持つ生体情報を利用した本人認証（バイオメトリクス認証）が重要とされてきており、中でも指紋認証は、低コストで比較的容易に導入・運用ができ、認証精度も向上していることから、最も広く普及している認証方法です。
パスワード入力等を意識することなく、自身の指を使い簡単かつ確実に本人認証を行うことができます。

●ファイル暗号化

指紋による本人認証に加え、PC内のデータを暗号化しておくことで、安全性をさらに高めることができます。USB暗号キー（デバイス内に格納してあるキー）を使用しての暗号化・復号化が可能ですので、暗号キーを覚える必要がなく、簡単な操作で処理が行えます。
また、データ削除の際に「シュレッダー削除」機能をお使いいただくことで、データを二度と復元できないように削除でき、PC廃棄後の情報漏洩対策としてもご利用いただけます。

Technology

●ラインセンサー指紋認証

指紋の読み取りにラインセンサーを用いることで、デバイスの小型化（USBへの搭載）を実現しました。また、デバイス（C4-Fingered専用USBキー）内のユーザ情報や指紋情報は、C4S暗号で暗号化処理し、格納しています。
さらに、デバイス内には暗号化キーも格納されており、暗号キーの入力なしに暗号化・復号化処理を行うことができます。

●C4S搭載

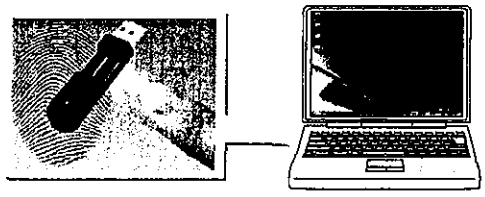
指紋データおよびファイルの暗号化には、高速・安全を誇る純国産暗号化技術"C4S"を採用しています。C4Sは、マルチプラットフォームを基本とし、強固にデータを守りながらも、高速な処理でストレスなく暗号化処理を行います。

C4Fingered

C4-Fingeredの機能

■指紋認証によるログオン

本人のみが持つ指紋で認証を行い、PCへのログオンを行います。パスワードを忘れることや、ICカード等の紛失・盗難の心配をすることなく、確実な本人認証で高いセキュリティを確保します。



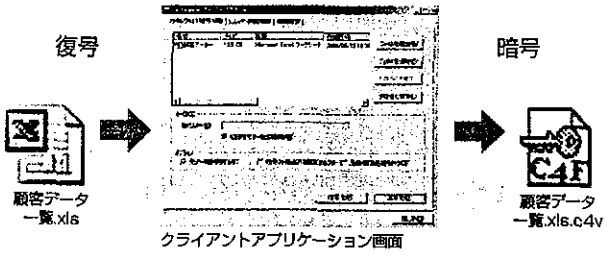
■指紋認証による スクリーンロック・スクリーンセーバーロック解除

スクリーンロックまたはスクリーンセーバーロック解除を指紋認証で行います。ちょっとした離席の際も、第三者によるPCの不正利用を防ぎます。

■ファイルプロテクト

フォルダやファイルの暗号化…簡単操作でデータを暗号化・復号化処理でき、重要な情報を守ります。

暗号書庫…データを圧縮して暗号化し、異なるドライブのフォルダやファイルも同一書庫へ格納し管理できます。



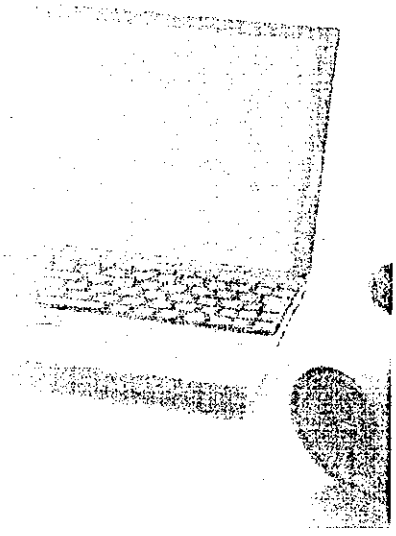
クライアントアプリケーション画面

■シュレッダー削除

復元ソフトを使用しても、データを二度と復元することができないように削除します。

■指紋認証による 管理アプリケーション（C4-Fingered）の起動

C4-Fingeredの発行や設定変更を行う「管理アプリケーション」の起動には、管理者の指紋認証が必要となるため、管理者以外の人物にむやみに設定変更されることがなく、高いセキュリティレベルを維持できます。



対応OS	Microsoft® Windows® 2000 日本語版 Microsoft® Windows® XP 日本語版

標準価格(税別)

商品名	価格
C4-Fingered アプリケーション （管理アプリケーション、クライアントアプリケーション）	¥149,800
C4-Fingered 専用USBキー	オープン価格

※ストラップもあります。(オプション)

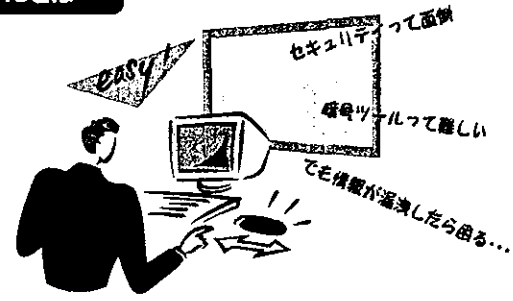
http://www.focus-s.com

販売元 Focus Systems
Bring Computer Solutions into Focus
株式会社フォーカスシステムズ
新規事業推進室
〒141-0022 東京都品川区東五反田1-23-1　フォーカス五反田第2ビル
TEL. 03-5420-3659　FAX. 03-5420-3634
E-mail prom@focus-s.com

こんな問題を解決します

- 社内セキュリティ対策として何かはじめたい。
- 難しい操作はできない。でもパソコンのデータは守りたい。
- Windowsのログオン、毎回毎回入力するのは面倒。
- 外に持ち出すノートパソコン 、置忘れや盗難にあったら情報漏洩?
- 経理情報、人事情報、査定報告に業務方針、会議等の離席時に見られてしまわないか。
- 本社と支社の月次報告、添付ファイルが盗み見られることはないのか。
- ファイルサーバや共有パソコンの研究データや個人情報、人に見せるわけにはいかない。

C4Uとは・・・



こういう方のための簡単暗号ツールです!!

簡単高度なセキュリティ

初回暗号フォルダ設定後、ユーザの操作はC4Uキーの抜きさしのみです。
暗号鍵の長さは自由に設定できます。(2048bitまで)
専用USBキーにはアラジンジャパン社のeTokenを採用。
コンパクトなボディに耐タンパ性を備えた制御チップを搭載、
暗号キーを安全に格納するデバイスです。

自由のC4Uキー再発行システム

紛失等による再発行は、C4Uキーの発行時に設定した複数個のリカバリキーをそろえてはじめて可能となる新しいシステムを提供しています。

高性能の暗号エンジン

C4Uの鍵となる暗号エンジンは最先端暗号化テクノロジー C4Sを採用しています。
C4Sは可変長鍵による強さ、機器に負荷をかけないスピードを持つ優れた純国産の暗号技術です。またそのエンジンの軽さのため汎用機から携帯電話まであらゆる場面に利用できるマルチプラットフォームを実現しました。
「誰でもできるファイルセキュリティ」をコンセプトに開発されたC4Uでは、この強力な暗号エンジンを簡単操作でご利用いただくことができます。

Confidence
Clever
Chaos
Crypto System

C4U Ver.2

ている人だけが使える。
ているだけで使える。

操作はキーの抜きさしだけ

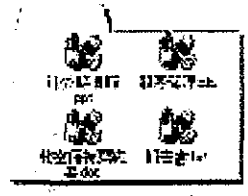
Ⅰ.ログオン・ログオフ機能

PC起動時にC4Uキーを
さすだけでログオンします。

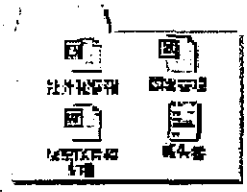
※機能Ⅰにおいて、Windows®98SE、Windows® MEは一部利用制限がございます。

C4Uキーを抜くだけで、
ログオフします。

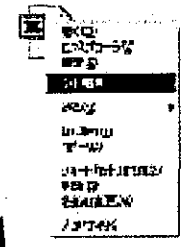
Ⅱ.自動暗号・復号機能



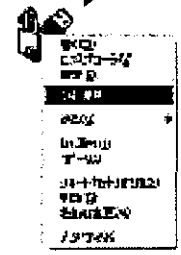
C4Uキーを抜きさしだけで指定されたフォルダ内のファイルが全て暗号・復号されます。



Ⅲ.手動暗号・復号機能



C4Uキーがさしてあれば右クリックで指定したファイルを自由に暗号・復号できます。



Ⅳ.改竄チェック機能

復号時には改竄されていないか確認します。

※暗号化されたファイルはC4Uキーがなければ開くことができません。

※これらの機能は組み合わせてお使いいただくことができます。
※1つのC4Uキーで複数のフォルダを指定することができます。
※1つのPCで複数のC4Uキーを使い分けることができます。

Price

◎C4Uアプリケーション CDセット……¥149,800／1セット
（鍵管理1ライセンス、クライアントフリーライセンス）
◎C4U専用USBキー……¥88,600／1セット（10本）
◎旧VersionからVer.2へのUpdate（USBキー はそのままご利用いただけます）…¥25,000／1セット

〔対応OS〕 Windows®98SE / Windows® Me / Windows®2000 / Windows® XP/ Windows® Server 2003（32bit版のみ）

URL:http://www.focus-s.com

開発元

Focus Systems
株式会社 フォーカスシステムズ
〒141-0022 東京都品川区東五反田1-4-1 ハニー五反田第2ビル
TEL:03-5421-1071　FAX:03-5421-1019
E-mail: c4@focus-s.com

2004-01

FIPS PUB 140-1 Test Result Details

Results of FIPS 140-1 Specified Tests on sample1

data: c4s(1Mbyte)

//1-20000

The monobit test	X=	9973	pass	(pass if 9654 <X <10346)
The poker test	X=	12.864	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2455	2579	pass	(pass if 2267 <X <2733)
2	1279	1158	pass	(pass if 1079 <X <1421)
3	636	621	pass	(pass if 502 <X <748)
4	326	306	pass	(pass if 223 <X <402)
5	166	186	pass	(pass if 90 <X <223)
6+	139	151	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//1000001-1020000

The monobit test	X=	10050	pass	(pass if 9654 <X <10346)
The poker test	X=	11.5264	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2554	2550	pass	(pass if 2267 <X <2733)
2	1283	1301	pass	(pass if 1079 <X <1421)
3	651	617	pass	(pass if 502 <X <748)
4	312	294	pass	(pass if 223 <X <402)
5	127	167	pass	(pass if 90 <X <223)
6+	145	142	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//2000001-2020000

The monobit test	X=	9987	pass	(pass if 9654 <X <10346)
The poker test	X=	20.5952	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2501	2509	pass	(pass if 2267 <X <2733)
2	1239	1216	pass	(pass if 1079 <X <1421)
3	615	640	pass	(pass if 502 <X <748)
4	336	337	pass	(pass if 223 <X <402)
5	160	165	pass	(pass if 90 <X <223)
6+	151	135	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//3000001-3020000

The monobit test	X=	9869	pass	(pass if 9654 <X <10346)
The poker test	X=	15.3856	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2481	2521	pass	(pass if 2267 <X <2733)
2	1227	1251	pass	(pass if 1079 <X <1421)
3	647	636	pass	(pass if 502 <X <748)
4	332	297	pass	(pass if 223 <X <402)
5	160	155	pass	(pass if 90 <X <223)
6+	157	144	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//4000001-4020000

The monobit test	X=	10048	pass	(pass if 9654 <X <10346)
The poker test	X=	17.0176	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2511	2462	pass	(pass if 2267 <X <2733)
2	1219	1242	pass	(pass if 1079 <X <1421)
3	612	624	pass	(pass if 502 <X <748)
4	316	335	pass	(pass if 223 <X <402)
5	172	143	pass	(pass if 90 <X <223)
6+	150	173	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

FIPS PUB 140-1 Test Result Details

Results of FIPS 140-1 Specified Tests on sample2

data: c4s(2Mbyte)

//1-20000

The monobit test	X=	9973	pass	(pass if 9654 <X <10346)
The poker test	X=	12.864	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2455	2579	pass	(pass if 2267 <X <2733)
2	1279	1158	pass	(pass if 1079 <X <1421)
3	636	621	pass	(pass if 502 <X <748)
4	326	306	pass	(pass if 223 <X <402)
5	166	186	pass	(pass if 90 <X <223)
6+	139	151	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//2000001-2020000

The monobit test	X=	9987	pass	(pass if 9654 <X <10346)
The poker test	X=	20.5952	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2501	2509	pass	(pass if 2267 <X <2733)
2	1239	1216	pass	(pass if 1079 <X <1421)
3	615	640	pass	(pass if 502 <X <748)
4	336	337	pass	(pass if 223 <X <402)
5	160	165	pass	(pass if 90 <X <223)
6+	151	135	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//4000001-4020000

The monobit test	X=	10048	pass	(pass if 9654 <X <10346)
The poker test	X=	17.0176	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2511	2462	pass	(pass if 2267 <X <2733)
2	1219	1242	pass	(pass if 1079 <X <1421)
3	612	624	pass	(pass if 502 <X <748)
4	316	335	pass	(pass if 223 <X <402)
5	172	143	pass	(pass if 90 <X <223)
6+	150	173	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//6000001-6020000

The monobit test	X=	10025	pass	(pass if 9654 <X <10346)
The poker test	X=	18.8864	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2497	2426	pass	(pass if 2267 <X <2733)
2	1278	1294	pass	(pass if 1079 <X <1421)
3	584	641	pass	(pass if 502 <X <748)
4	315	340	pass	(pass if 223 <X <402)
5	160	161	pass	(pass if 90 <X <223)
6+	161	132	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//8000001-8020000

The monobit test	X=	10045	pass	(pass if 9654 <X <10346)
The poker test	X=	19.8912	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2489	2499	pass	(pass if 2267 <X <2733)
2	1252	1221	pass	(pass if 1079 <X <1421)
3	601	604	pass	(pass if 502 <X <748)
4	313	303	pass	(pass if 223 <X <402)
5	161	157	pass	(pass if 90 <X <223)
6+	157	189	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

FIPS PUB 140-1 Test Result Details

Results of FIPS 140-1 Specified Tests on sample3

data: c4s(1Mbyte)

//1-20000

The monobit test	X=	10105	pass	(pass if 9654 <X <10346)
The poker test	X=	18.0224	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2539	2479	pass	(pass if 2267 <X <2733)
2	1246	1249	pass	(pass if 1079 <X <1421)
3	625	639	pass	(pass if 502 <X <748)
4	302	316	pass	(pass if 223 <X <402)
5	154	166	pass	(pass if 90 <X <223)
6+	144	160	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//1000001-1020000

The monobit test	X=	9914	pass	(pass if 9654 <X <10346)
The poker test	X=	11.0336	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2417	2483	pass	(pass if 2267 <X <2733)
2	1285	1277	pass	(pass if 1079 <X <1421)
3	657	616	pass	(pass if 502 <X <748)
4	304	313	pass	(pass if 223 <X <402)
5	161	145	pass	(pass if 90 <X <223)
6+	159	150	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//2000001-2020000

The monobit test	X=	9938	pass	(pass if 9654 <X <10346)
The poker test	X=	10.752	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2518	2480	pass	(pass if 2267 <X <2733)
2	1232	1314	pass	(pass if 1079 <X <1421)
3	630	612	pass	(pass if 502 <X <748)
4	311	300	pass	(pass if 223 <X <402)
5	156	165	pass	(pass if 90 <X <223)
6+	166	142	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//3000001-3020000

The monobit test	X=	9946	pass	(pass if 9654 <X <10346)
The poker test	X=	14.4192	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2479	2492	pass	(pass if 2267 <X <2733)
2	1208	1246	pass	(pass if 1079 <X <1421)
3	628	606	pass	(pass if 502 <X <748)
4	307	303	pass	(pass if 223 <X <402)
5	169	150	pass	(pass if 90 <X <223)
6+	170	165	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//4000001-4020000

The monobit test	X=	9991	pass	(pass if 9654 <X <10346)
The poker test	X=	17.7728	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2476	2467	pass	(pass if 2267 <X <2733)
2	1236	1249	pass	(pass if 1079 <X <1421)
3	604	600	pass	(pass if 502 <X <748)
4	316	309	pass	(pass if 223 <X <402)
5	150	164	pass	(pass if 90 <X <223)
6+	173	166	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

FIPS PUB 140-1 Test Result Details

Results of FIPS 140-1 Specified Tests on sample4

data: c4s(2Mbyte)

//1-20000

The monobit test	X=	10105	pass	(pass if 9654 <X <10346)
The poker test	X=	18.0224	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2539	2479	pass	(pass if 2267 <X <2733)
2	1246	1249	pass	(pass if 1079 <X <1421)
3	625	639	pass	(pass if 502 <X <748)
4	302	316	pass	(pass if 223 <X <402)
5	154	166	pass	(pass if 90 <X <223)
6+	144	160	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//2000001-2020000

The monobit test	X=	9938	pass	(pass if 9654 <X <10346)
The poker test	X=	10.752	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2518	2480	pass	(pass if 2267 <X <2733)
2	1232	1314	pass	(pass if 1079 <X <1421)
3	630	612	pass	(pass if 502 <X <748)
4	311	300	pass	(pass if 223 <X <402)
5	156	165	pass	(pass if 90 <X <223)
6+	166	142	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//4000001-4020000

The monobit test	X=	9991	pass	(pass if 9654 <X <10346)
The poker test	X=	17.7728	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2476	2467	pass	(pass if 2267 <X <2733)
2	1236	1249	pass	(pass if 1079 <X <1421)
3	604	600	pass	(pass if 502 <X <748)
4	316	309	pass	(pass if 223 <X <402)
5	150	164	pass	(pass if 90 <X <223)
6+	173	166	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//6000001-6020000

The monobit test	X=	10003	pass	(pass if 9654 <X <10346)
The poker test	X=	17.3696	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2371	2408	pass	(pass if 2267 <X <2733)
2	1291	1263	pass	(pass if 1079 <X <1421)
3	635	622	pass	(pass if 502 <X <748)
4	302	299	pass	(pass if 223 <X <402)
5	165	159	pass	(pass if 90 <X <223)
6+	159	173	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//8000001-8020000

The monobit test	X=	9929	pass	(pass if 9654 <X <10346)
The poker test	X=	12.4672	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2559	2571	pass	(pass if 2267 <X <2733)
2	1248	1316	pass	(pass if 1079 <X <1421)
3	617	587	pass	(pass if 502 <X <748)
4	323	287	pass	(pass if 223 <X <402)
5	179	152	pass	(pass if 90 <X <223)
6+	140	152	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

参考資料:

eToken R2 のタンパー機能について

Aladdin
SECURING THE GLOBAL VILLAGE

(株)アラジンジャパン

1. はじめに

eToken R2

eToken R2 は、内部のメモリに構成した秘密領域を極めて堅牢に保護し、悪意あるアタックや解析から強固にプロテクトするセキュリティ・デバイスです。

eToken が備えているこの機能のように、ある領域に格納した秘密情報（たとえばアプリケーションで使用する暗号キー、PKI における秘密鍵など、機密を要するデータ）をプロテクトする機能をタンパー機能と言います。本資料では、eToken R2 がこのクラスで最高のタンパー機能をどのように実現しているかについて、いくつかの観点からその概要を説明します。

2. タンパー性に関係するハードウェアの基本機能

2.1 内臓暗号処理機能

eToken R2 は、DES-X（120bit キー）対称アルゴリズムを搭載しています。この機能は、eToken R2 内部で、すべての秘密データの暗号化、およびユーザ認証プロトコルにおけるチャレンジレスポンスの仕組みに使用しています。またこの機能は、PC 上の情報を保護するための暗号化/復号化エンジンとしても使用することができます。

2.2 RNG ベースのチャレンジレスポンス機能

eToken R2 はランダム・シードをベースにした擬似乱数発生機構を内臓しています。これと上の DES-X 機能により、ログイン制御を行います。つまりパスワードを検証するときは、eToken R2 内でランダムなチャレンジ値を発生させ、PC に送ります。レスポンス値は格納しているパスワードと比較されます。これにより、eToken は二因子認証による確実なユーザ認証を行います。

3. 秘密情報に対するプロテクション

eToken R2 のタンパー性は上のハードウェア基本機能をベースにしていますが、以下に主要な観点からどのように秘密領域をプロテクトしているかを説明します。

3.1 チップに対するプロテクション

eToken R2 は、物理的にはセキュア化されたマイクロコントローラと EEPROM で構成されています。EEPROM にはすべてのデータが格納されますが、ユーザ・データや暗号鍵など、秘密領域の内容はマイクロコントローラに格納されたキーにより、DES-X で暗号化されて EEPROM に格納されます。これらのキー（120bit 長）は、如何なる方法によっても、読み出したりアクセスしたりすることはできません。

3.2 USB データ・トラフィックに対するプロテクション

eToken R2 へのログインが成功することによってのみ、秘密領域へのアクセスが可能になることに加え、そのデータのトラフィックは常に暗号化されます。トラフィックの暗号化はログイン時に乱数発生機構で生成される 120bit 長のセッションキーを使用して DES-X アルゴリズムで行われます。

したがって、USB 信号ラインをスニッファー装置で解析しようとしても、またハウジングをはずしメモリからUSB に至る回路上を同様の装置で解析しようとしてもできません。

3.3 アクセスに対するプロテクション

eToken R2 内の秘密データの書き込みと使用は、eToken へログインすることによりのみ、可能になります。ログインは、きわめて高度なセキュリティレベルが確保できるチャレンジレスポンス方式によってのみ可能であり、加えてチャレンジ値は上記のように乱数発生機構により発生させています。このように、レスポンス値は毎回ランダムに変化することに加え、DES-X で暗号化していますので、ハウジングを破壊して開けてもパスワードが判明することはありません。

3.4 制御に対するプロテクション

eToken R2 のマイクロコントローラで使用するファームウェアは、アクセスしたり取り出したりすることができません。このため、ハウジングを破壊して開け、直接マイクロコントローラ・チップになんらかの機器を接続して解析し、悪意あるものに書き換えて動作そのものを変えようとしても不可能です。

3.5 タンパー・エビデント

タンパー・エビデントとは、”改ざんした、あるいは改ざんを試みた痕跡が物理的に残る作りになっていること“ を指します。悪意から未然に防ぐ意味で、セキュリティ・デバイスでは重要な要求事項の一つになっています。

eToken R2 は、改ざんや解析のため内部にアクセスするには、ハウジングを破壊しない限り行うことができず、また一旦破壊すると復元することはできません。 なおプラスチック製のハウジングにはガラス繊維が混入されており、頑丈なだけでなく痕跡を残させることにも役立っております。

さらには、このような構造なのでタンパー性に加え、IP X8-IEC 529 の防水規格をも満たしており、持ち歩くことによる水との接触の可能性に対しても考慮が払われております。

医療情報のセキュリティに関する研究

分担研究者　山本　隆一　　東京大学大学院情報学環　助教授

研究要旨　HIV ネットにおいてセキュリティの確保が重要なことは論を待たないが、今後の HIV ネットにおいていずれは診療情報システムとのリンクが問題になってくる。本研究では診療情報システム自体のセキュリティの基準を検討、考察した。なお、本研究の成果は研究者が主査となって作成した、厚労省の医療情報システムの安全管理ガイドラインに反映されている。

A．研究目的

高度情報通信社会の急速な進展、個人情報保護への関心の高まり、データ保護に関するＥＵ指令や HIPAA 法に関連した米国規則など、諸外国のプライバシー保護、セキュリティの規制の変化等から、我が国においても保健医療分野での個人情報保護のあり方に関して、国際動向や現在のセキュリティ技術水準を踏まえた一定の方向性を示すことが緊急かつ重大な課題となっている。また国会においては、平成 15 年 5 月に個人情報保護関連 5 法案が成立し、平成 17 年 4 月の実施が決定されており、ガイドラインの作成が一層重要性をおびている。さらに、電子化情報は二次利用が容易で、大量の情報を容易に扱いうることから、情報システムの安全管理がきわめて重要になっている。

本研究は、HIV ネットが将来、参加病院の診療情報システムと有機的にリンクする要求が高まることに配慮し、高度なセキュリティと個人情報保護が求められる HIV ネットと診療情報システムがリンク可能な程度のセキュリティを保てるかどうかを検討することを目的としている。本年は HIV ネットと接続を前提としたものではなく、基礎的な診療情報システムのセキュリティ基準について検討することとする。

B．研究方法

（1）個人情報保護法に関する指針等の安全管理義務にあたる部分の要件抽出。

個人情報保護法（関連 3 法）は対象分野を限定しないために、きわめて抽象的で、

情報セキュリティのように、あくまでも相対的な評価しかなしえない対策においては基準を定めることが難しい。そのために、関係省府は指針を定めている。本研究では経済産業省の指針と厚生労働省の医療・介護関係事業者における個人情報の適切な取り扱いに関するガイドラインを精査し、要件を抽出した。

（２）これまでに公表されている医療情報システムの安全管理に係る指針の調査

平成６年に医用画像の電子保存を容認する通知が出され、その際に基準と指針が作成されている。また平成１１年にいわゆる電子保存の容認通知が出され、基準と指針が作成された。また海外では HIPAA 法の実施にあたって、米国厚生省が security standards を省令として定めている。これらを精査し、要件を抽出した。

（３）個人情報保護法に対応する情報システムの安全管理指針の作成

（２）で抽出した要件の中で、電子保存等の特別な行為に依存しない一般的な安全管理対策を基礎として、（１）で抽出した２指針の要件を加味し、安全管理指針を作成した。

C．研究結果

（１）個人情報保護法に関する指針等の安全管理義務にあたる部分の要件抽出。

いずれの指針も組織的、人的、技術的、物理的対策を求めており、リスク分析を基礎に体系的な対策をとることを求めている。また、やや具体的なレベルとしてはアクセス制限、アクセス記録の採取と保存を求めている。その一方でアクセス制限やアクセス記録の基礎となる利用者の識別に関しては言及されていない。また平成１７年３月末時点で公表されているＱアンドＡでは個人情報をコンピュータシステムへ入力する際に、入力やの記録は必ずしも必要でないとするなど、矛盾した対応も見られる。

（２）これまでに公表されている医療情報システムの安全管理に係る指針の調査

平成６年の医用画像の電子保存の指針は、基準自体がほぼ技術的対策に限定して述べられていることもあって、技術仕様書といっても良いものであった。情報の完全性や可用性に関しては技術のみでも対策は不可能ではないが、機密性や情報主権の勘案など個人情報保護の観点からの安全管理対策は情報の利活用の場面でも保障される必要があり、技術だけでは達成できない。その意味ではこの指針は現時点では著しく不十分といわざるを得ない。

平成１１年の電子保存通知の際に作成された指針は技術と運用のバランスで安全管理を達成することを求めており、現実的な指針となっている。また組織的、人的、物理的対策にも言及はされている。しかしながら、技術面ではかなり厳格に中立的立場で書かれており、著しく具体性に欠ける。そのために、技術的対策と相補的に講じられるべき組織的、人的対策も、歯切れの悪い記載になっており、電子保存のように、ある程度技術力のある組織が実施する、いわば特殊な状況での指針としては機能するが、個人情報保護法への対応のように、医療情報システムを導入しているすべての医療機関が対応しなければならない状況では不適切と考えざるをえない。

米国の HIPAA Security Standards も国際的に見れば重要な安全管理基準ではあるが、Privacy Standards が医療情報全般を対象にして作成された汎用的なものであるのに比べて、Security Standards は HIPAA 法の一部である、オンライン診療報酬請求にかなり限定して定められたもので、また、内容は主にシステムのベンダー向けであり、抽象的である。米国では HIPAA 法の施行前はわが国ほどレセコン等の情報機器の導入は進んではなく、HIPAA 法のオンライン診療報酬請求の義務化に対して導入を行う医療機関が多いために、このような基準で機能するのであろうが、わが国のようにすでに７０％以上の医療機関に医療情報システムが導入している状況では、やはり具体性に欠けるといわざるを得ない。

なお、平成１４年にわが国では外部保存に関する通知が出され、基準と指針が作成されているが、安全管理に関しては、平成１１年の指針と大きく異なる点はないために、ここでは割愛する。

（３）個人情報保護法に対応する情報システムの安全管理指針の作成

（２）の結果から、平成１１年の電子保存に関する指針から電子保存を行うか否かにかかわらず安全管理上必要な項目を抽出し、（１）の２つの指針の要件と和をとり、指針を作成した。指針の全文は付録として添付するが、概要をいかに示す。

１．方針の制定と公表

電子保存の指針では透明性の確保は触れられていなかったが、個人情報保護の指針で、特に厚労省指針では透明性の確保は重視されており、追加した。

２．情報の取り扱いの把握とリスク分析

リスク分析は安全管理上もっとも重要な初期ステップであるが、医療機関はスタッ

フの信頼関係を基礎に医療業務を行っている関係からか、リスク分析が不得意な傾向にある。したがってリスクを例示し、取り組み易さを目指した。以下の亜項目にわけて示している。

２．１　取り扱い情報の把握

２．２　リスク分析

３．組織的安全管理対策（体制、運用管理規程）

体制は適応する組織の形態に大きく依存するし、運用管理規程も物理的な対策や技術的対策と相補的であり、具体的な記述が困難な部分であった。運用管理規程は物理的対策や技術的対策に応じて具体化されるべきもので、対応表形式で整備することが望まれる。

４．物理的安全対策

情報システムの物理的安全対策は建物の立地条件から考慮されるべきであるが、すでに大多数の医療機関に導入されている医療情報システムの安全管理を扱う指針であることから、管理区分の設定と施錠、入退管理のみを記載した。

５．技術的安全対策

平成１１年の電子保存に関する指針が技術的中立性を基本としたために全体として理解しがたいものであったことを踏まえ、具体的な技術要素にできるだけ触れることとした。利用者の識別及び認証、情報の区分管理とアクセス権限の管理、アクセスの記録（アクセスログ）、不正ソフトウェア対策の４項に分けて指針を示した。もっとも重要な利用者の識別および認証においては、パスワード認証、生体計測認証、ICカード等の所持情報のそれぞれ技術的な特徴と採用する際の運用上の留意点を示した。また技術要素は現時点でのコストも勘案して記載したために、精度は高いものの高額のために、一般的な医療機関では採用が困難なものは除いて指針を示している。

６．人的安全対策

医療機関の職員に対する対策と、第三者、特に情報システムの保守等の委託契約に対して言及している。

７．情報の破棄

個人情報保護法が存在しなくても医療従事者の守秘義務の観点から重要な項目であるが、これまで存在する医療分野の指針では積極的に触れられていなかった項目である。内容は単純であるが、指針として明記した。

８．情報システムの改造と保守

医療情報システムにとっては重要な項目であり、６の人的安全対策の委託契約と一

部重複するが、しばしば実施される点数改定や制度の変更による情報システムの改造は、いわば日常茶飯事であり、それだけに指針として明示する必要がある。あくまでも医療機関が責務を全うするという観点から監督責任に重点をおいた指針とした。

9．外部と個人情報を含む医療情報を交換する場合の安全管理

オンラインメインテナンスやネットワークを利用した医療連携が相当する。現時点でそれほど普及しているわけではないが、維持コストや連携密度を上げる観点から今後急速に普及すると思われるために、特に指針を示した。ただし、ＡＳＰ型のレセコンや電子カルテに代表されるオンラインの外部保存に関しては、単なる安全管理だけではなく、情報の二次利用の制限や責任分担などさまざまな問題があるために、安全管理の指針としては対象外としている。

D．考察

HIV ネットは全国一律な HIV 感染者のケアと研究の促進のために設置された先進的な取り組みであり、先進的である故から安全管理はきわめて厳重に行われている。厳重であること自体はまったく問題はないが、厳重であるために、適切な情報の利用に多大な労力が必要となり、本来促進されるべき患者等のプライバシーを十分保護した状態での情報の利活用が十分促進されているとは言いがたい状況である。しかしHIV ネット設置時以降、情報の安全管理は技術的にも運用的にも研究が進み、適切な対策をとれば高度な安全管理と利活用の両立も不可能ではない。

HIV ネットにおいて情報を利活用する上でもっとも重要な点は各施設で用いているオーダリングシステム、電子カルテなどの病院情報システムとの連携であろう。しかし現時点ではこれはセキュリティやプライバシー保護の観点から実現されていない。これを実現するためにはHIV ネット自体のセキュリティポリシーの見直しも必要であるが、その前提として病院情報システム自体の安全管理が十分でなければならない。

本研究ではHIV ネットの将来の利活用の発展の基礎としての個人情報保護法の実施に対応した病院情報システムの安全管理のための要件を抽出し、指針を作成した。

これまでも医療情報システムの安全管理指針はまったくなかったわけではなく、平成６年の医用画像の電子保存容認通知に伴う基準と指針、平成１１年の診療録等の電子保存容認通知に伴う指針が存在した。しかしこれはいずれも、保存義務のある文書