情報セキュリティ　第一回レポート

C0115114 菅野路哉

6 月 1 日

1　平文

学籍番号から今回用いる平文を求める。平文は、学籍番号の数字部を 2 進数に直したものを 3 つ並べ、64bit で 0 埋めしたものである。

平文 0000000000000111000001101010101110000011010101011100000110101010

次に、**図 1** を使用して平文の転置を行う。

初期転置後の平文 0110000000100000000100110011111010110110001000100010001000100010011110

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

図 1　転置表

さらに、転置された平文を 32bit ずつに分割する。

転置後 32bit 分割された平文

左 01100000001000000001001100111110

右 11011000100010001000100010011110

2　鍵

今回は、鍵として以下を用いる。

10011111010101010101000001101000101100101001111011101010000111001

図 2 を使用して鍵の縮約転置を行う。

転置後の鍵 01110001010011101101100010110111000100100011111010010111

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

図 2　転置表

さらに、転置された鍵を 28bit ずつに分割する。

転置後分解

左 0111000101001110110110001011

右 0111000100100011111010010111

分割された鍵をそれぞれ回転左シフトし、再結合する。

回転左シフトされた値

1110001010011101101100010110

1110001001000111110100101110

再結合された値 111000101001110110110001011011100010010001111101001011 10

再結合された鍵を、**図 3** を使用して転置を行う。また、これを拡大鍵とする。

拡大鍵 110110100000011010111111001001101101100001110010

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

図 3　転置表

3　関数 F

分割された平文の右側と、拡大鍵を使用して関数 F の結果を求める。初めに、分割された平文の右側を**図 4** を使用して拡大転置を行う。その後、転置された平文と拡大鍵の排他的論理和を求める。求めたビット列を**図 5**、**図 6** の SBOX を参照して変換する。

SBOX による変換は、6bit に分割された値をそれぞれ SX の表に当てはめて計算する。分割された bit 列の外側の bit を取り、それを結合した値を行数、内側の値を列数に SBOX の値を参照する。

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

図 4　転置表

S1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

図 5　SBOX 表 (S1〜S4)

```
S5
   2 12  4  1  7 10 11  6  8  5  3 15 13  0 14  9
  14 11  2 12  4  7 13  1  5  0 15 10  3  9  8  6
   4  2  1 11 10 13  7  8 15  9 12  5  6  3  0 14
  11  8 12  7  1 14  2 13  6 15  0  9 10  4  5  3
S6
  12  1 10 15  9  2  6  8  0 13  3  4 14  7  5 11
  10 15  4  2  7 12  9  5  6  1 13 14  0 11  3  8
   9 14 15  5  2  8 12  3  7  0  4 10  1 13 11  6
   4  3  2 12  9  5 15 10 11 14  1  7  6  0  8 13
S7
   4 11  2 14 15  0  8 13  3 12  9  7  5 10  6  1
  13  0 11  7  4  9  1 10 14  3  5 12  2 15  8  6
   1  4 11 13 12  3  7 14 10 15  6  8  0  5  9  2
   6 11 13  8  1  4 10  7  9  5  0 15 14  2  3 12
S8
  13  2  8  4  6 15 11  1 10  9  3 14  5  0 12  7
   1 15 13  8 10  3  7  4 12  5  6 11  0 14  9  2
   7 11  4  1  9 12 14  2  0  6 10 13 15  3  5  8
   2  1 14  7  4 10  8 13 15 12  9  0  3  5  6 11
```

図 6　SBOX 表 (S5〜S8)

平文右 11011 0001 0001 0001 0001 0001 0011 110

転置された平文 011011 110001 010001 010001 010001 010001 010011 111101

拡大鍵 110110 100000 011010 111111 001001 101101 100001 110010

排他的論理和をとった値 101101 010001 001011 101110 011000 111100 110010 001111

SBOX によって出た値

S1 1

S2 12

S3 4

S4 13

S5 13

S6 11

S7 15

S8 4

SBOX で求めた数値をそれぞれ二進数に変換する。

0001 1100 0100 1101 1101 1011 1111 0100

この値をさらに**図 7** で転置を行った値が関数 F の値となる。

関数 F の値 10110011001111010011010001110011

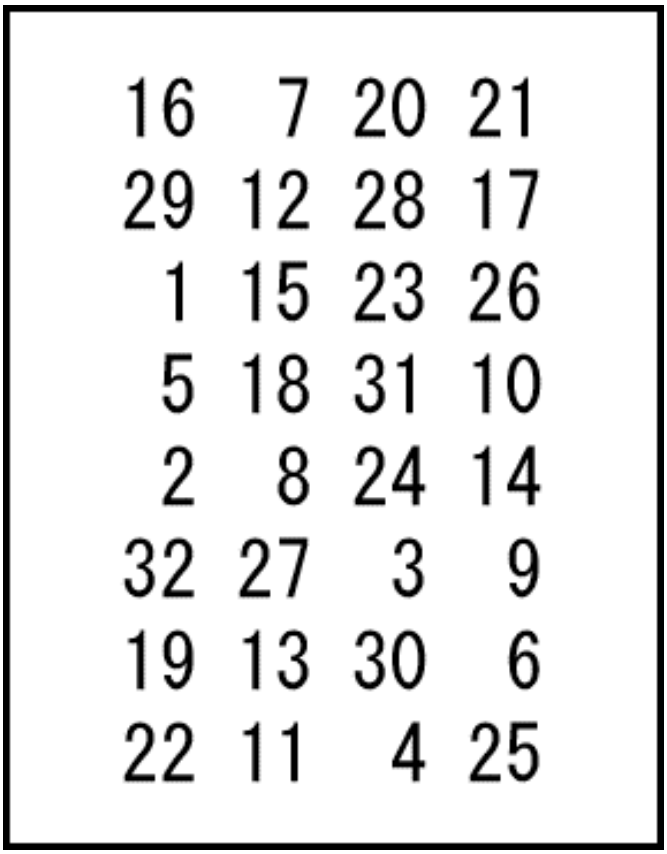

図 7　転置表

4　最終値

最後に、関数 F で求めた数値と、分割された平文の左側の排他的論理和を求める。

平文左 01100000001000000010011001111010

関数 F 10110011001111010011010001110011

最終値 11010011000111010001001000001001