軽量暗号、秘密分散法と組み込み機器における実装例

MCPC勉強会　2021年11月18日
株式会社エイチアイ 開発部開発三課 課長　鈴木隆元

自己紹介

2001年　木更津高専情報工学科卒業
2003年　日本大学文理学部応用数学科卒業
2003年　組み込み IT ベンチャーに就職
2010年　株式会社イーソルへ転職。RTOS の開発と機能安全プロセス構築に従事
2011年　もっと勉強しておけばよかった病をこじらせ、JAIST 社会人コースに入学
2015年　JAIST 修士課程修了（優秀修了生）。博士課程へ進学
2015年　株式会社エイチアイに転職
　　車載アプリケーション開発、セキュリティとネットワークの自社研究開発に従事

好きな言語: C, Python ,Lisp, AWK
専門: 組み込みシステム、オペレーティングシステム、リアルタイムスケジューリング、車載アプリケーション
JASAセキュリティ委員、情報処理学会、CSAJ、トリリオンノード研究会会員

主な著作、学会発表:
ARM9 評価ボードにLinuxを移植する / Interface 2009年10月号
ARM9 拡張子基盤をLinuxから活用する / Interface 2009年11月号
仮想サーバによるタスクの応答時間短縮手法 /鈴木隆元, 田中清史, 組み込みシステムシンポジウム 2016
T. Suzuki and K. Tanaka, "Execution Right Delegation: Beyond the Rate Monotonic' Proc. of the 32nd International Conference on Computers and Their Applications, 2017.
T. Suzuki and K. Tanaka, "Response Time Analysis of Execution Right Delegation Scheduling" Proceedings of Asia Pacific Conference on Robot IoT System Development and Platform (2020), 32-38, 2021-03-15
T.Suzuki and K.Tanaka, “Execution Right Delegation Scheduling Algorithm for Multiprocessor” IEEE 14th International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoC 2021)

所属紹介

会社名	株式会社エイチアイ （英語表記：HI CORPORATION）
本社所在地	東京都港区港南2丁目15番3号 品川インターシティC棟17階

Hack your problem and fix **I**t together
Hop On the rapid express **I**nto a vivid future
A **HI**p **CO**mpany that is so se**R**ious about your **P**roblems
Hoping our solutions **I**ncrease your value.
HIt the stars with our creations!

講演のターゲット

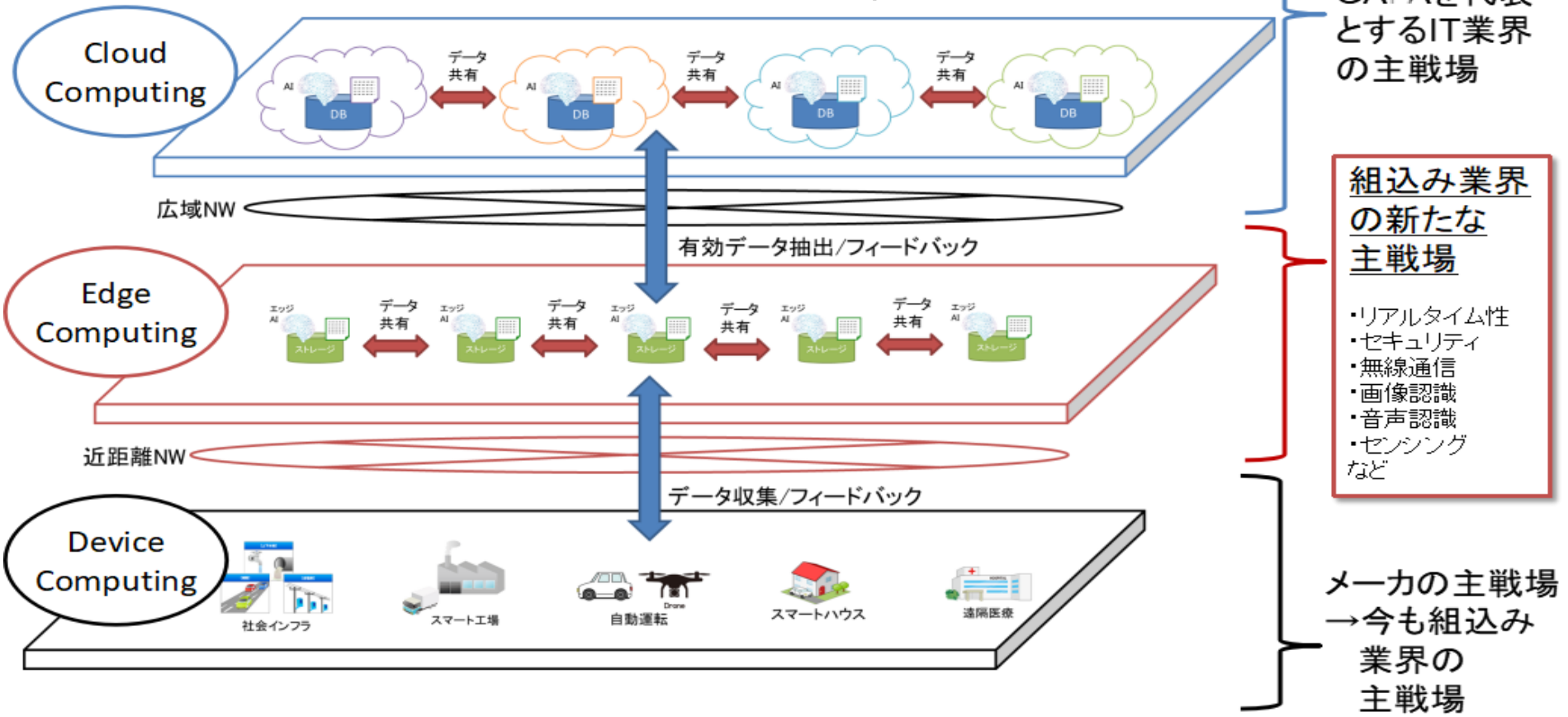
- IoT デバイスを扱っており、セキュリティに興味のある方
  - どういう手法があるか知りたい
  - 効率的な実装方法などのノウハウが知りたい
  - 扱ってるデバイスが非力過ぎてセキュリティ導入出来ません
  - 秘密分散て何ですか

Agenda

- イントロダクション
- 組み込み向け軽量暗号
- 秘密分散法
- IoTA ～ 組み込み機器での実装例

イントロダクション
～DX とセキュリティ～

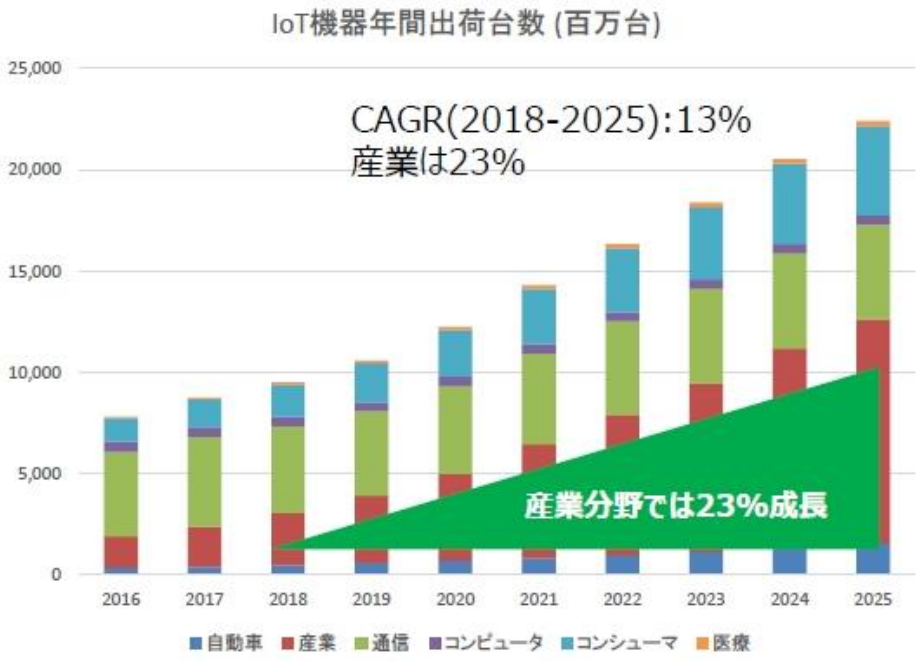
- Society 5.0 の実現　→　DX によるデータ活用
- データ自身が機密性、完全性、可用性を持つ必要性
- 官民の標準化拡大（ISO 21434, WP29）

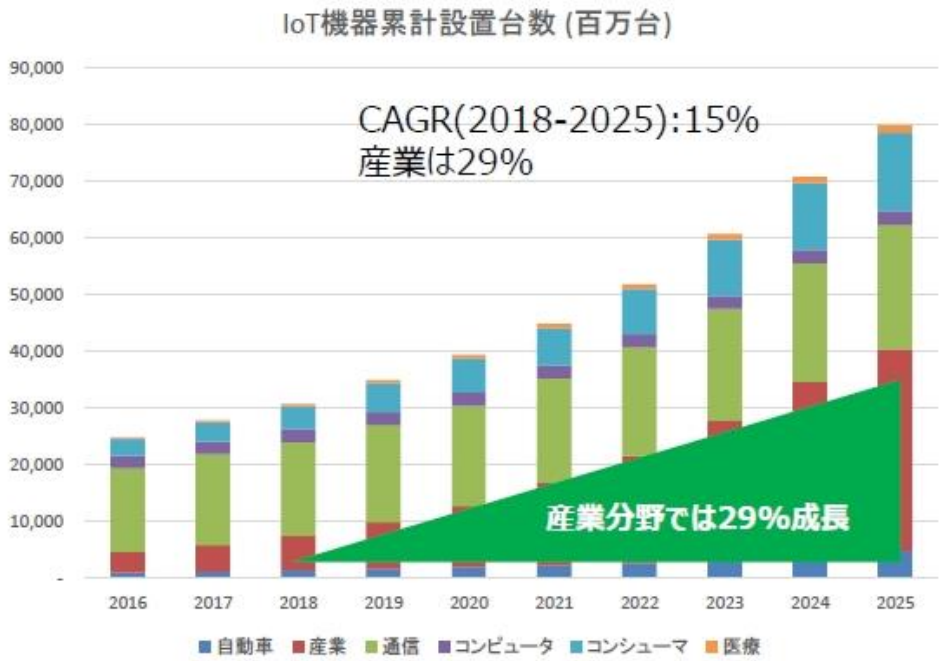


イントロダクション
～IoTデバイスの増加～

世界の分野別IoT機器出荷実績と予測

・IoTデバイスは2018年で年間約100億台、2025年には200億台強が出荷される見込み
・累計設置台数は2018年で300億台、2025年には800億台に達する見込み
・産業分野で大きく成長が見込まれる (通信分野には年間約15億台規模のスマフォが含まれている)



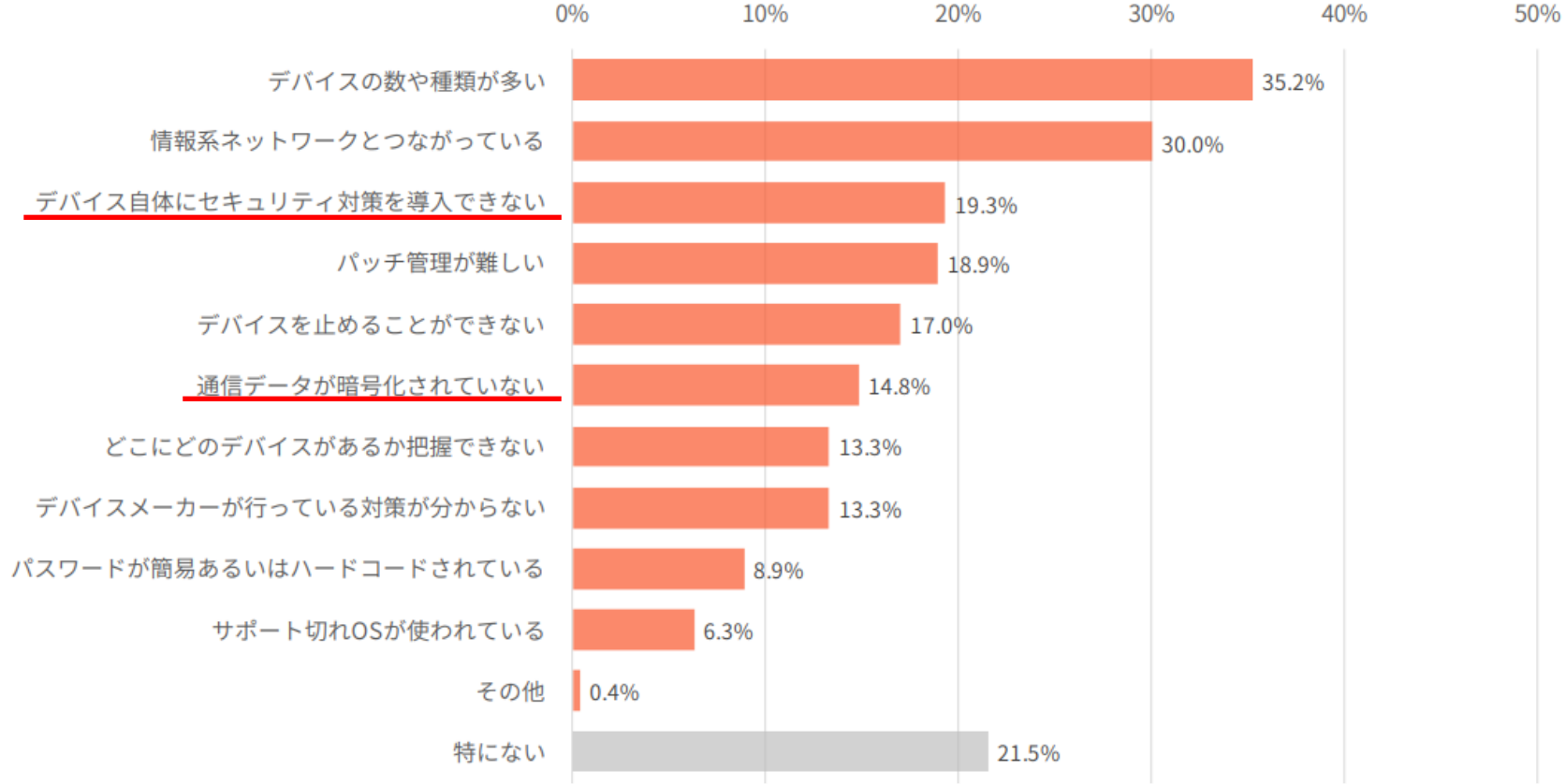


出所：IHS Markit

参考出展：https://www.sbbit.jp/article/cont1/36642

イントロダクション
～セキュリティ対策の課題～

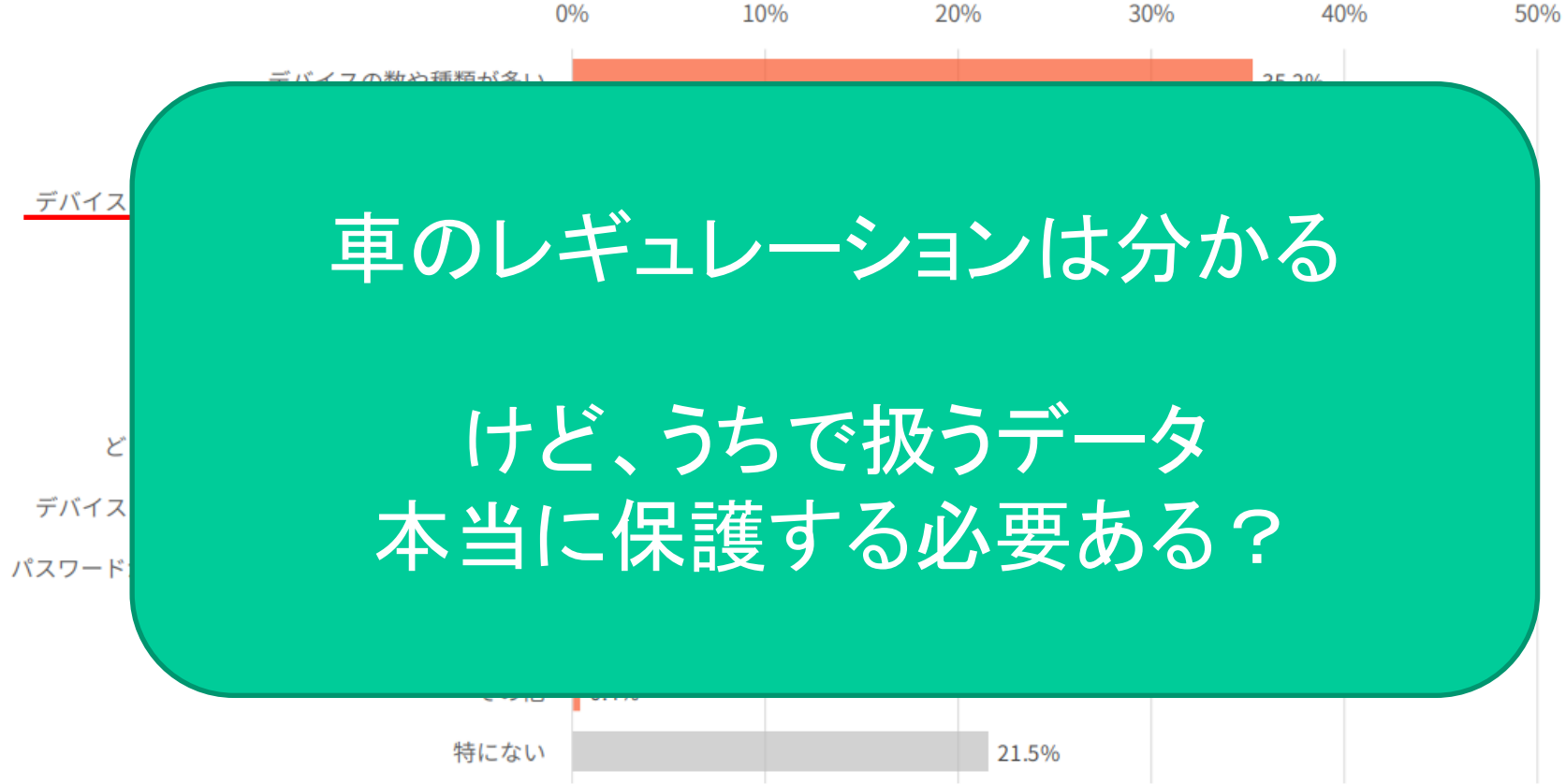
- 一方で、IoT 機器のセキュリティ対策には課題が多い
  - セキュリティ対策の不在 … 19.3%
  - 通信データの非暗号化 … 14.8%



参考出展：IoT/OT サイバーセキュリティジャパンサーベイ2020 年版 https://start.paloaltonetworks.jp/iot-ot-japan-survey-2020.html

イントロダクション
～セキュリティ対策の課題～

- 一方で、IoT 機器のセキュリティ対策には課題が多い
  - セキュリティ対策の不在 … 19.3%
  - 通信データの非暗号化 … 14.8%

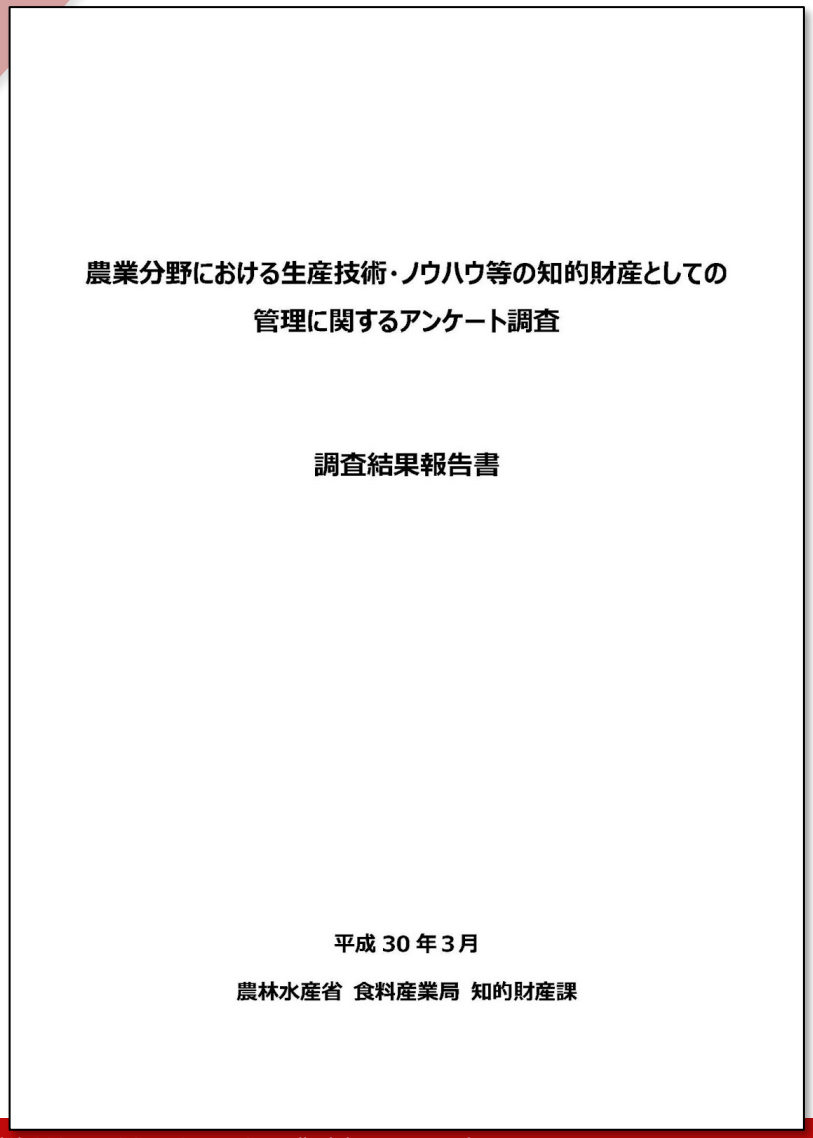


車のレギュレーションは分かる

けど、うちで扱うデータ
本当に保護する必要ある？

参考出展：IoT/OT サイバーセキュリティジャパンサーベイ2020 年版 https://start.paloaltonetworks.jp/iot-ot-japan-survey-2020.html

イントロダクション
～農業の例～



農業分野における生産技術・ノウハウ等の知的財産としての
管理に関するアンケート調査

調査結果報告書

平成 30 年３月

農林水産省 食料産業局 知的財産課

https://www.maff.go.jp/j/kanbo/tizai/brand/knowhow.html

イントロダクション
～農業の例～

図１　どのようなものをノウハウとして認識しているか。

図２　どのようにノウハウを獲得しているか。

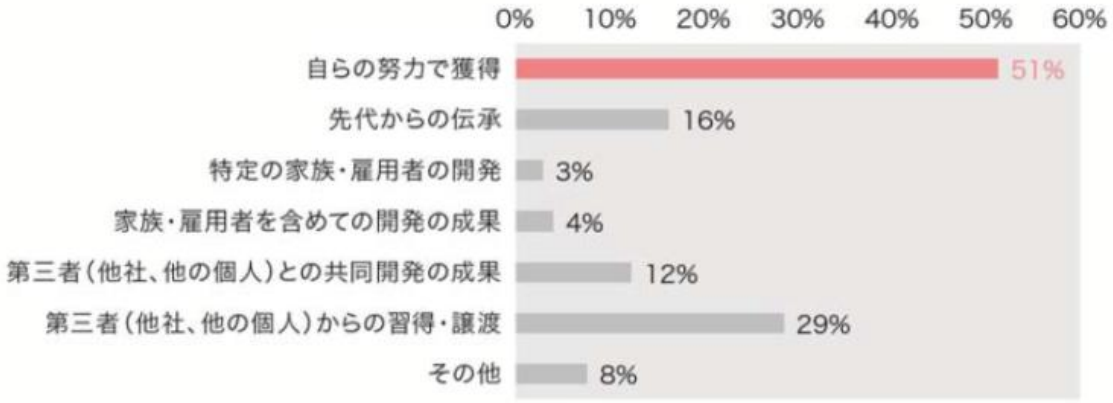
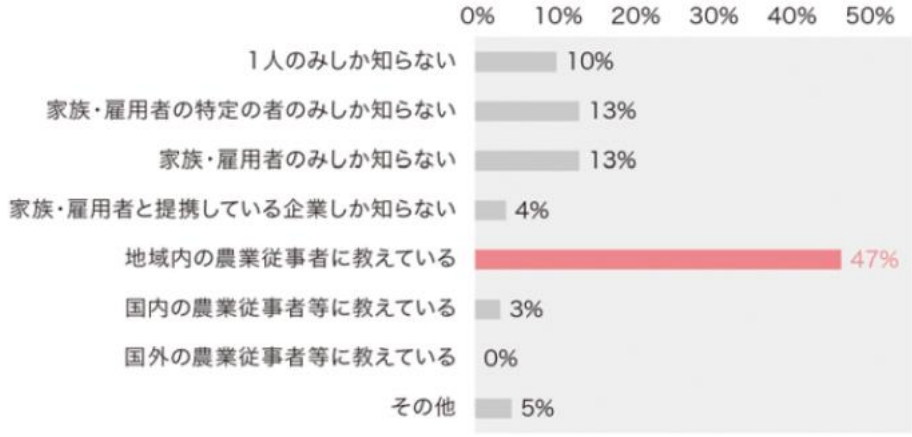


図３　どの範囲までノウハウを共有しているか。
図３　どの範囲までノウハウを共有しているか。



イントロダクション
～農業の例～

図４　ノウハウが財産的価値を有する可能性があることを認識しているか。

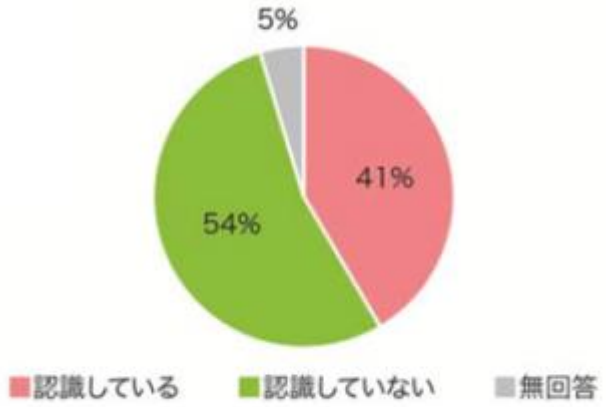


図５　ノウハウを管理しているか。

イントロダクション
～農業の例～

【調査実施概要】

農業者が有する農産物の生産方法に関する**ノウハウ等**は、我が国が誇る高品質な農産物の生産を支える**重要な財産**であり、今後農産物の競争力を強化するにあたりその重要性は更に高まっている。
農林水産省では、そのような農産物の生産に関するノウハウ等をいかに**保護**し、活用を促していくかについて、関係機関と協力して検討を進めており、今般、検討を進めるにあたり、農業現場における生産技術に関するノウハウ等の管理の実態を把握するとともに、ノウハウが流出した事例等の情報を収集するため、本アンケート調査を実施した。

イントロダクション
～平文通信による漏洩の例～

```
hal@A120015A: ~/prj/iota/iota/application/mosquitto-master
hal@A120015A:~/prj/iota/iota/application/mosquitto-master$ echo -n test_OK | mosquitto_pub
-t 'iota/test' -s -u hicorp -P iota123 -r -p 1883 -h 192.168.1.31
```

```
hal@joshua:~ $ sudo tcpdump -i wlan0 port 1883 -A -w cap.bin
tcpdump: listening on wlan0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C16 packets captured
16 packets received by filter
0 packets dropped by kernel
hal@joshua:~ $ hexdump ./cap.bin -C | head -n 25 | tail
000000f0  07 5b bf 9c 05 74 07 fc  31 3e 50 10 02 01 5c 71  |.[...t..1>P...\q|
00000100  00 00 4f 5a c8 60 96 0f  00 00 55 00 00 00 55 00  |..OZ.`....U...U.|
00000110  00 00 b8 27 eb 6e ee 43  e4 70 b8 fa a6 13 08 00  |...'.n.C.p......|
00000120  45 00 00 47 85 df 40 00  80 06 f1 5c c0 a8 01 05  |E..G..@....\....|
00000130  c0 a8 01 1f c8 47 07 5b  bf 9c 05 74 07 fc 31 3e  |     G.[   t  1>|
00000140  50 18 02 01 25 2c 00 00  10 1d 00 04 4d 51 54 54  |P...%,......MQTT|
00000150  04 c2 00 3c 00 00 00 06  68 69 63 6f 72 70 00 07  |...<....hicorp..|
00000160  69 6f 74 61 31 32 33 4f  5a c8 60 1a 10 00 00 36  |iota123OZ.`....6|
00000170  00 00 00 36 00 00 00 e4  70 b8 fa a6 13 b8 27 eb  |...6....p.....'.|
00000180  6e ee 43 08 00 45 00 00  28 9f 6c 40 00 40 06 17  |n.C..E..(.l@.@..|
hal@joshua:~ $ hexdump ./cap.bin -C | head -n 60 | tail
00000320  5c 39 00 00 4f 5a c8 60  d8 fa 00 00 4a 00 00 00  |\9..OZ.`....J...|
00000330  4a 00 00 00 e4 70 b8 fa  a6 13 b8 27 eb 6e ee 43  |J....p.....'.n.C|
00000340  08 00 45 00 00 3c 9f 70  40 00 40 06 17 d7 c0 a8  |..E..<.p@.@.....|
00000350  01 1f c0 a8 01 05 07 5b  c8 47 07 fc 31 47 bf 9c  |.......[.G..1G..|
00000360  05 a3 50 18 03 ec 18 cc  00 00 31 12 00 09 69 6f  |..P.......1...io|
00000370  74 61 2f 74 65 73 74 74  65 73 74 5f 4f 4b 4f 5a  |ta/testtest_OKOZ|
00000380  c8 60 e0 10 01 00 38 00  00 00 38 00 00 00 b8 27  |.`....8...8....'|
00000390  eb 6e ee 43 e4 70 b8 fa  a6 13 08 00 45 00 00 2a  |.n.C.p......E..*|
000003a0  85 e2 40 00 80 06 f1 76  c0 a8 01 05 c0 a8 01 1f  |..@....v........|
000003b0  c8 47 07 5b bf 9c 05 a3  07 fc 31 5b 50 18 02 01  |.G.[......1[P...|
hal@joshua:~ $
```

イントロダクション
～まとめ～

- セキュリティ対策のニーズが拡大
  - DX
  - ISO 21434 などの標準

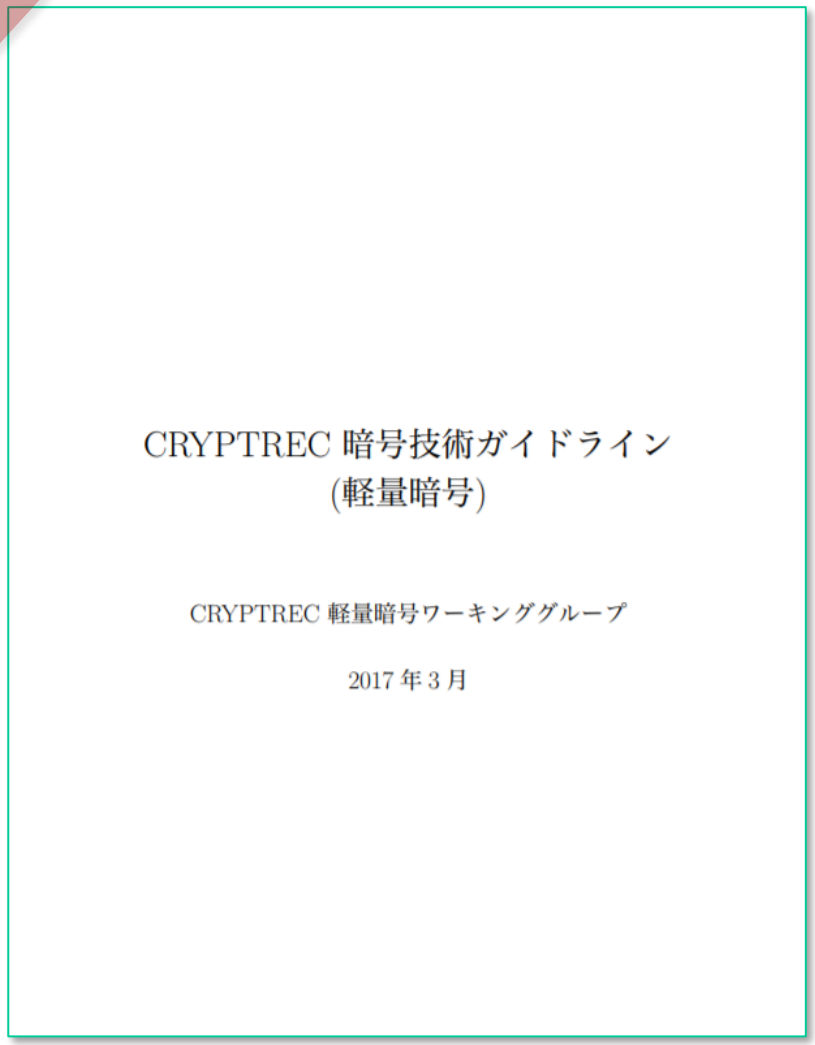
- データ収集を行う IoT デバイスへの対策の重要性
  - セキュリティ対策されてないことによるリスク
  - 低 CPU、小フットプリントの制約

- セキュリティ対策のニーズ拡大（再度）
  - 農業の例

Agenda

- イントロダクション
- 組み込み向け軽量暗号
- 秘密分散法
- IoTA ～ 組み込み機器での実装例

軽量暗号


CRYPTREC 暗号技術ガイドライン
(軽量暗号)

CRYPTREC 軽量暗号ワーキンググループ

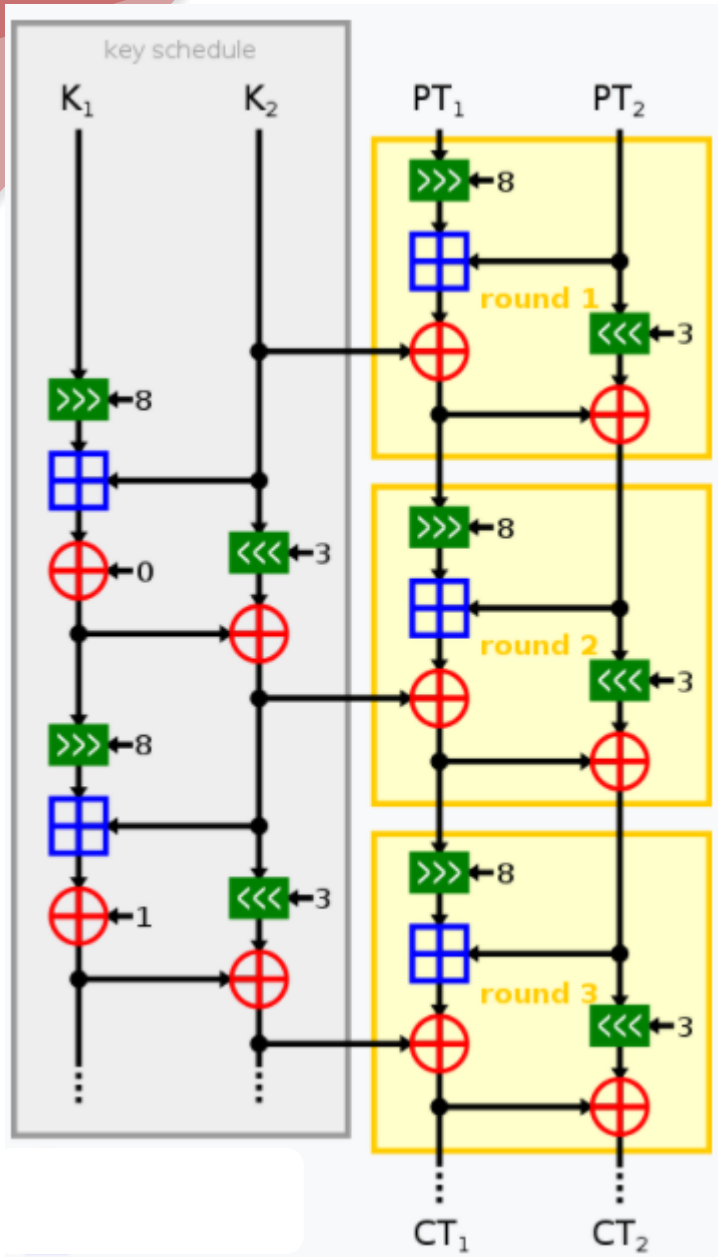
2017 年 3 月

IoT機器向けの”軽量”な暗号実装

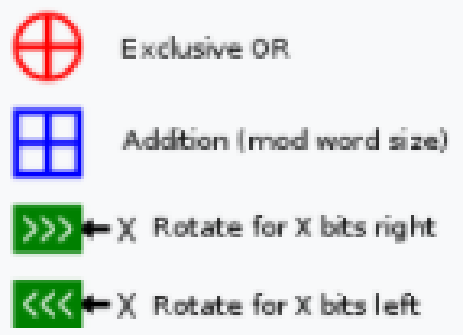
- HW
  - 回路規模
  - 消費電力量
  - レイテンシ
- SW
  - メモリサイズ（ROM/RAM）

https://www.cryptrec.go.jp/report/cryptrec-gl-2003-2016jp.pdf

軽量暗号 ～SPECK～



- NSA が 2013年に発表
- 非常に小さな ROM サイズで実装可能な軽量ブロック暗号
- 平文と鍵をブロックに分けて，ブロック単位の加減算や排他的論理和の演算を複数ラウンド行う



画像出展：https://en.wikipedia.org/wiki/Speck_(cipher)

軽量暗号
～SPECK vs AES の評価結果～

- CRYPTREC の評価は RL78 (16bit CPU) での評価
  - この評価環境では、SPECK と AES は同等の性能
- トリリオンノード Leafony STM32 (ARM Cortex-M, 32bit) と AVR (8bit) で評価してみた

トリリオンノード研究会

https://trillion-node.org/

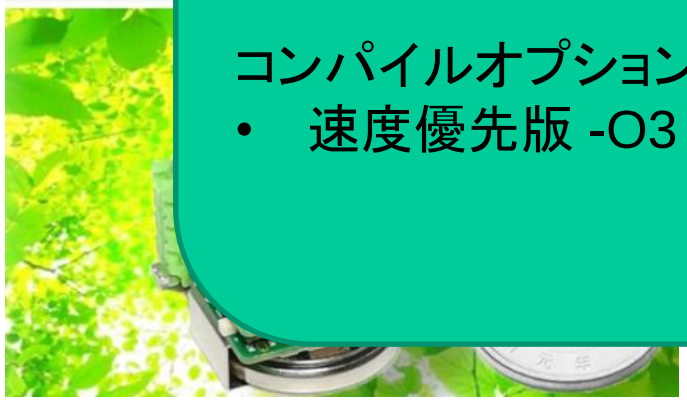
Leafony AVR MCU
(ATmega328P)

Leafony STM32
(Cortex-M4)

軽量暗号
～SPECK vs AES の評価結果～

- CRYPTRE
  - この評
- トリリオ
  AVR (8b

トリリオ



https://trillion-node.org/

評価パターン

実装方法：
- 速度優先版 vs フットプリント優先版
  - ・ループ展開の有無 (SPECK, AES 共)
  - ・データテーブル保持の有無（AESのみ）

コンパイルオプション：
- 速度優先版 -O3 vs フットプリント優先版 -Os

Leafony AVR MCU
(ATmega328P)

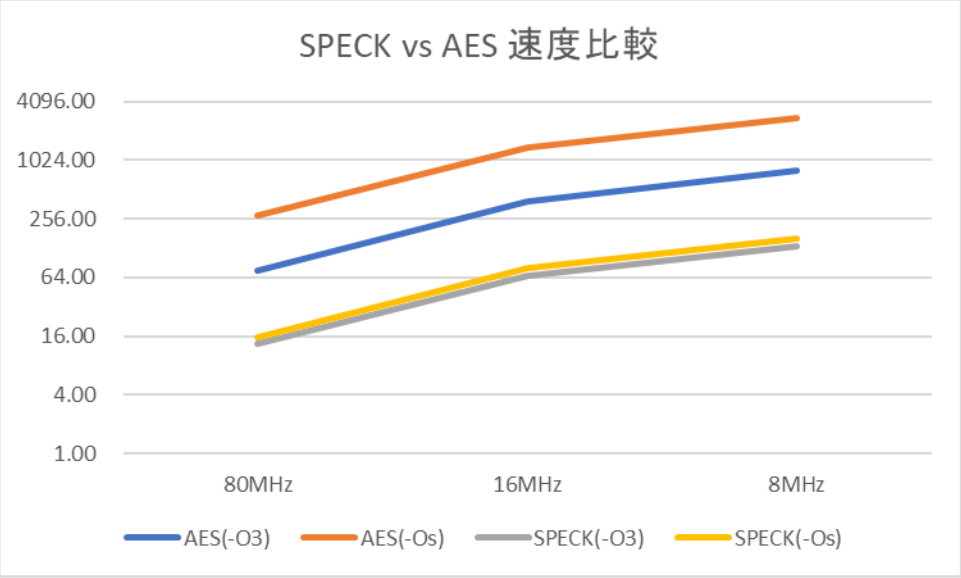
Leafony STM32
(Cortex-M4)

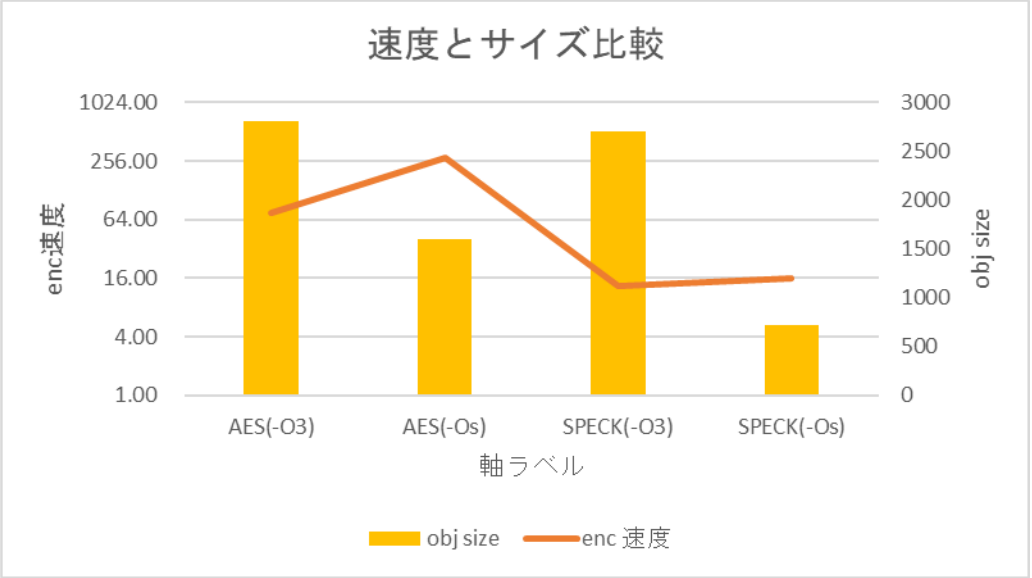
軽量暗号
～SPECK vs AES の評価結果（STM32)～

	Leafony STM32 MCU Cortex-M4		80MHz		16MHz		8MHz		
	暗号化実装	opt	enc(usec)	dec(usec)	enc(usec)	dec(usec)	enc(usec)	dec(usec)	obj size
AES	フットプリント優先版	-O3	75.98	74.74	387.79	381.69	791.21	780.27	2803
	フットプリント優先版	-Os	274.84	273.51	1378.79	1372.90	2759.69	2760.04	1599
	速度優先版	-O3	108.59	106.80	552.15	542.88	1130.84	1111.88	4763
	速度優先版	-Os	82.56	82.67	416.70	416.69	845.68	830.48	3827
SPECK	フットプリント優先版	-O3	13.20	13.20	66.20	66.20	132.88	132.87	2704
	フットプリント優先版	-Os	15.78	15.78	79.12	79.11	158.77	158.76	722
	速度優先版	-O3	19.20	19.17	96.40	96.26	193.76	193.50	6300
	速度優先版	-Os	18.94	18.90	95.08	94.87	191.14	190.72	4506

軽量暗号
～SPECK vs AES の評価結果（STM32)～

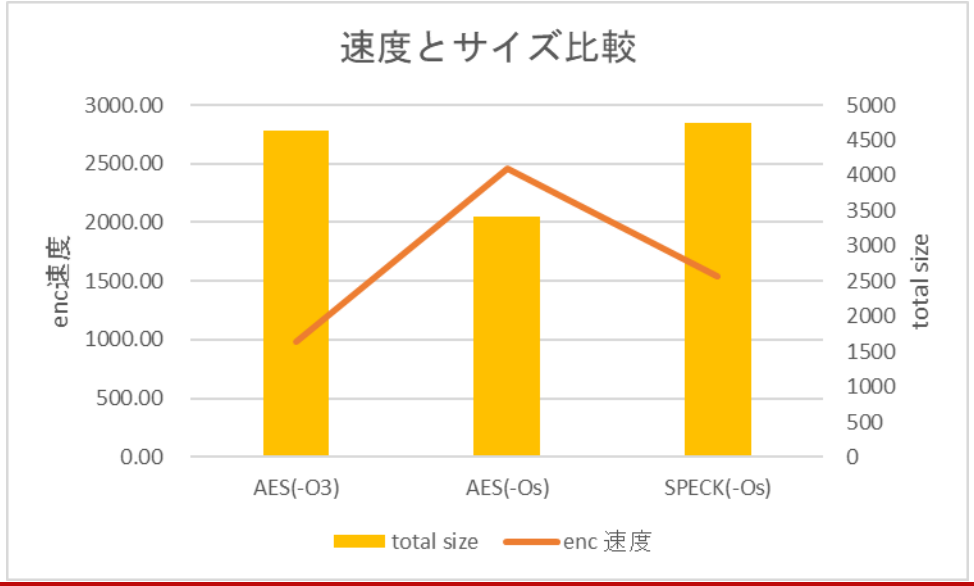
	Leafony STM32 MCU Cortex-M4		80MHz		16MHz		8MHz		
	暗号化実装	opt	enc(usec)	dec(usec)	enc(usec)	dec(usec)	enc(usec)	dec(usec)	obj size
AES	フットプリント優先版	-O3	75.98	74.74	387.79	381.69	791.21	780.27	2803
	フットプリント優先版	-Os	274.84	273.51	1378.79	1372.90	2759.69	2760.04	1599
	速度優先版	-O3	108.59	106.80	552.15	542.88	1130.84	1111.88	4763
	速度優先版	-Os	82.56	82.67	416.70	416.69	845.68	830.48	3827
SPECK	フットプリント優先版	-O3	13.20	13.20	66.20	66.20	132.88	132.87	2704
	フットプリント優先版	-Os	15.78	15.78	79.12	79.11	158.77	158.76	722
	速度優先版	-O3	19.20	19.17	96.40	96.26	193.76	193.50	6300
	速度優先版	-Os	18.94	18.90	95.08	94.87	191.14	190.72	4506





軽量暗号
～SPECK vs AES の評価結果 (AVR)～

	Leafony AVR MCU	ATmega 328P 8MHz			
暗号化実装		opt	enc(usec)	dec(usec)	total size
AES	フットプリント優先版	-O3	979.35	979.35	4628
	フットプリント優先版	-Os	2453.06	2453.07	3406
	速度優先版	-O3	969.41	969.42	5052
	速度優先版	-Os	1130.08	1130.09	4358
SPECK	フットプリント優先版	-O3	N/A	N/A	6042
	フットプリント優先版	-Os	1539.01	1539.02	4740
	速度優先版	-O3	N/A	N/A	11214
	速度優先版	-Os	1361.71	1361.71	10692



軽量暗号
まとめ

- STM32 において SPECK は、速度、フットプリント共に有利
  - AES は HW アクセラレーションが無いときつい
  - SPECK であれば、より多くのデータ送信が現実的な時間で可能に

軽量暗号
まとめ

- STM32 において SPECK は、速度、フットプリント共に有利
  - AES は HW アクセラレーションが無いときつい
  - SPECK であれば、より多くのデータ送信が現実的な時間で可能に

- AES、SPECK 共に速度優先版は必ずしも早くない
  - ART（キャッシュ）が2KByte※ ぽいのでメモリアクセスが増え逆効果
    - -O2/3 の場合は暗号コアの処理ステップが 8KByte を超える

軽量暗号
まとめ

- STM32 において SPECK は、速度、フットプリント共に有利
  - AES は HW アクセラレーションが無いときつい
  - SPECK であれば、より多くのデータ送信が現実的な時間で可能に

- AES、SPECK 共に速度優先版は必ずしも早くない
  - ART（キャッシュ）が2KByte※ ぽいのでメモリアクセスが増え逆効果
    - -O2/3 の場合は暗号コアの処理ステップが 8KByte を超える

- AVR においては SPECK は十分な速度を出せない
  - SPECK は理論上は 16bit、実装上は 64bit の単位でデータを処理
  - 8bit CPU の AVR では向かない

軽量暗号
まとめ

- STM32 において SPECK は、速度、フットプリント共に有利
  - AES は HW アクセラレーションが無いときつい
  - SPE
- AES、
  - AR
    -
- AVR (
  - SPE
  - 8bi

重要なこと

最適化を意識したパフォーマンス計測、ちゃんとやりましょう

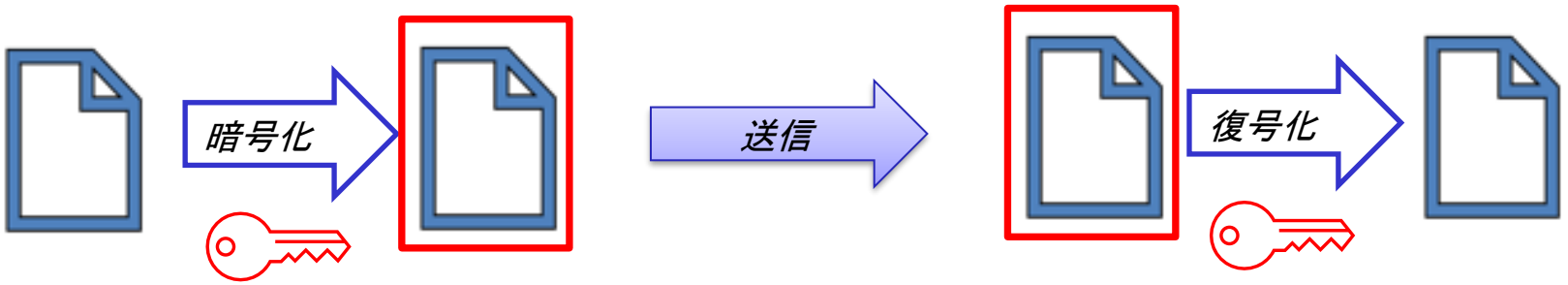
IoT プログラミングにおいては
軽い≒早い≒ CPU消費量が少ない≒ SDGs的に正義

Agenda

- イントロダクション
- 組み込み向け軽量暗号
- 秘密分散法
- IoTA ～ 組み込み機器での実装例

秘密分散法
～背景～

- 通常の暗号化と送信
  - ファイルを一定の長さのブロックに分割し、鍵を用いて暗号化
  - 暗号ファイルと鍵を送信
  - 暗号ファイルの一部と鍵を傍受されるだけでも、情報が漏洩してしまう
  - 鍵の管理が面倒（同一の鍵を再利用してしまうことも多い）

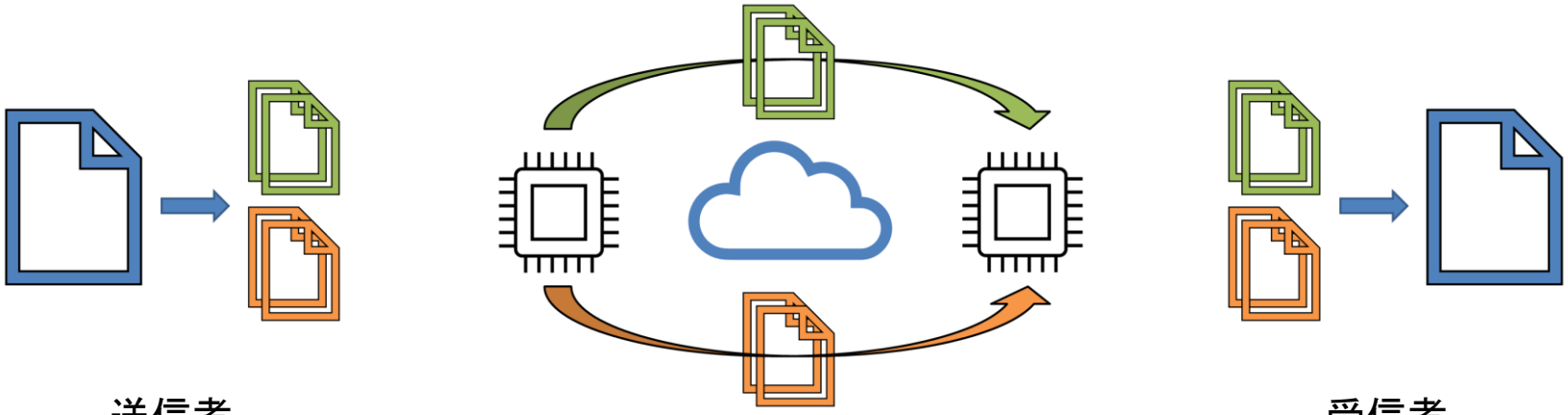


送信者　　受信者

少し前の事例：内閣官房のデータ流出 サイバー攻撃対応の訓練情報流出判明
https://www3.nhk.or.jp/news/html/20210602/k10013064581000.html

秘密分散法
～特徴～

- 秘密分散と送信
  - ファイルを一定の長さの分散片に分割する
  - 分散片を一定の個数傍受されない限り、情報が漏洩しない
  - 鍵の管理が不要（な運用も可能）



秘密分散法
～AONT～

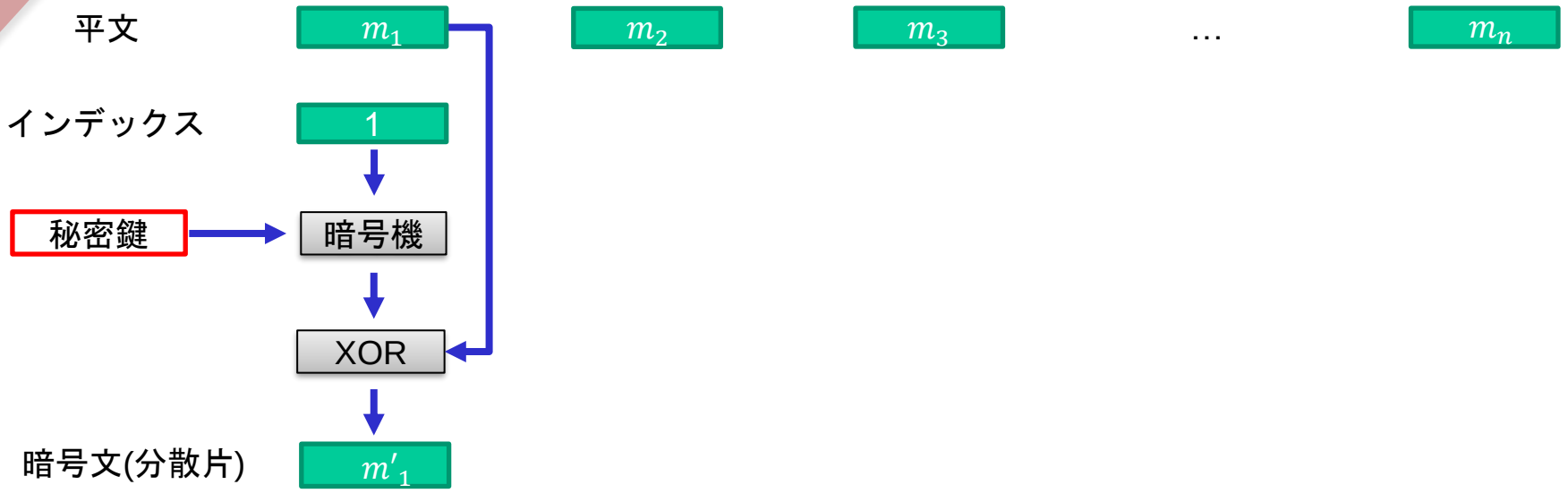
- Rivest の All or Nothing Transform
  - 平文をブロックに区切ってブロックのインデックスに**秘密鍵**を用い暗号化を行い，元のデータと排他的論理和をとって，変換する（分散片を得る）
  - 暗号化を行った**秘密鍵**に対して，各変換データ（分散片）と排他的論理和をとって、変換する
  - すべての変換データ（分散片）を集めると、**秘密鍵**を復元して元のデータを復元できる

秘密分散法
～AONT 分散化～

平文 m_1 m_2 m_3 … m_n

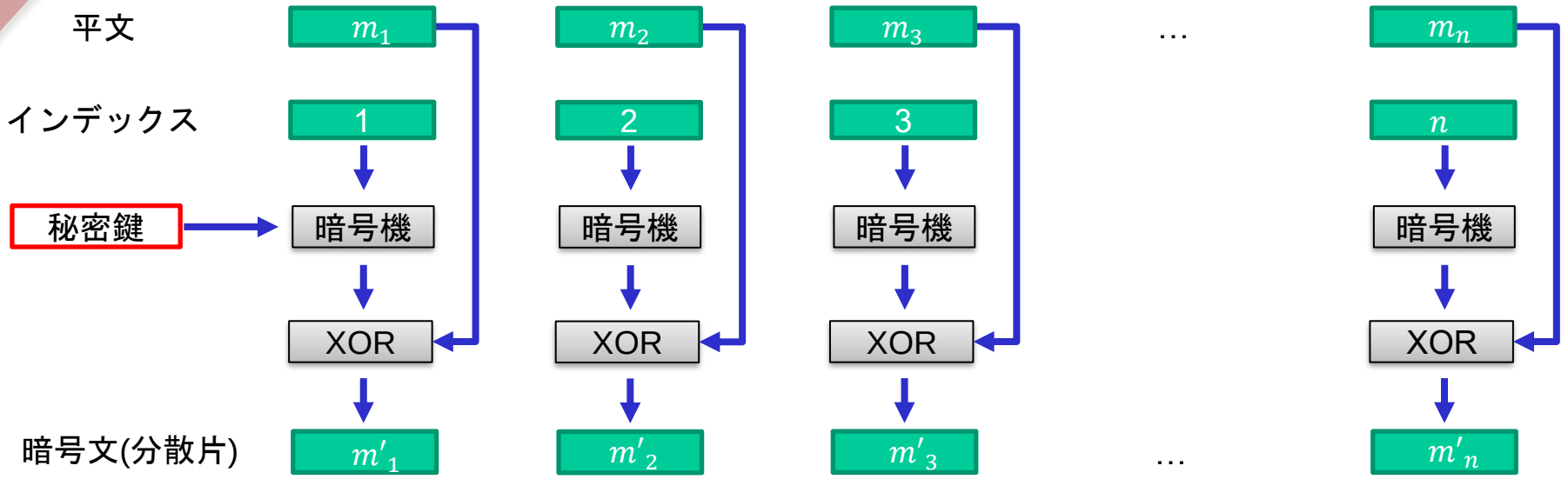
平文を $m_1, m_2, \ldots, m_n$ に分割する

秘密分散法
～AONT 分散化～



分割したインデックス i を秘密鍵を用いて暗号器へ入れる
結果を平文 m_i と XOR し、分散片 m'_i とする

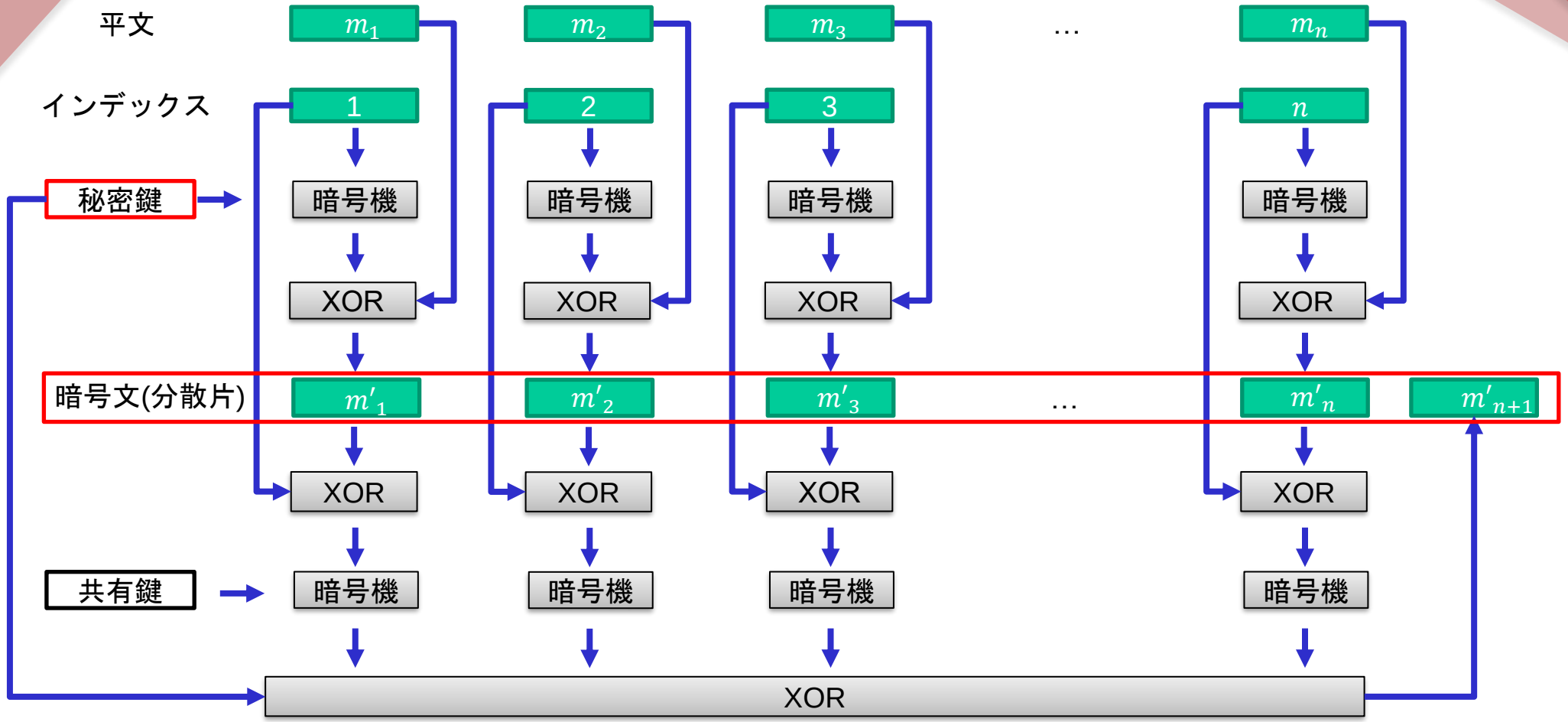
秘密分散法
～AONT 分散化～



同様の処理をm_n まで行う

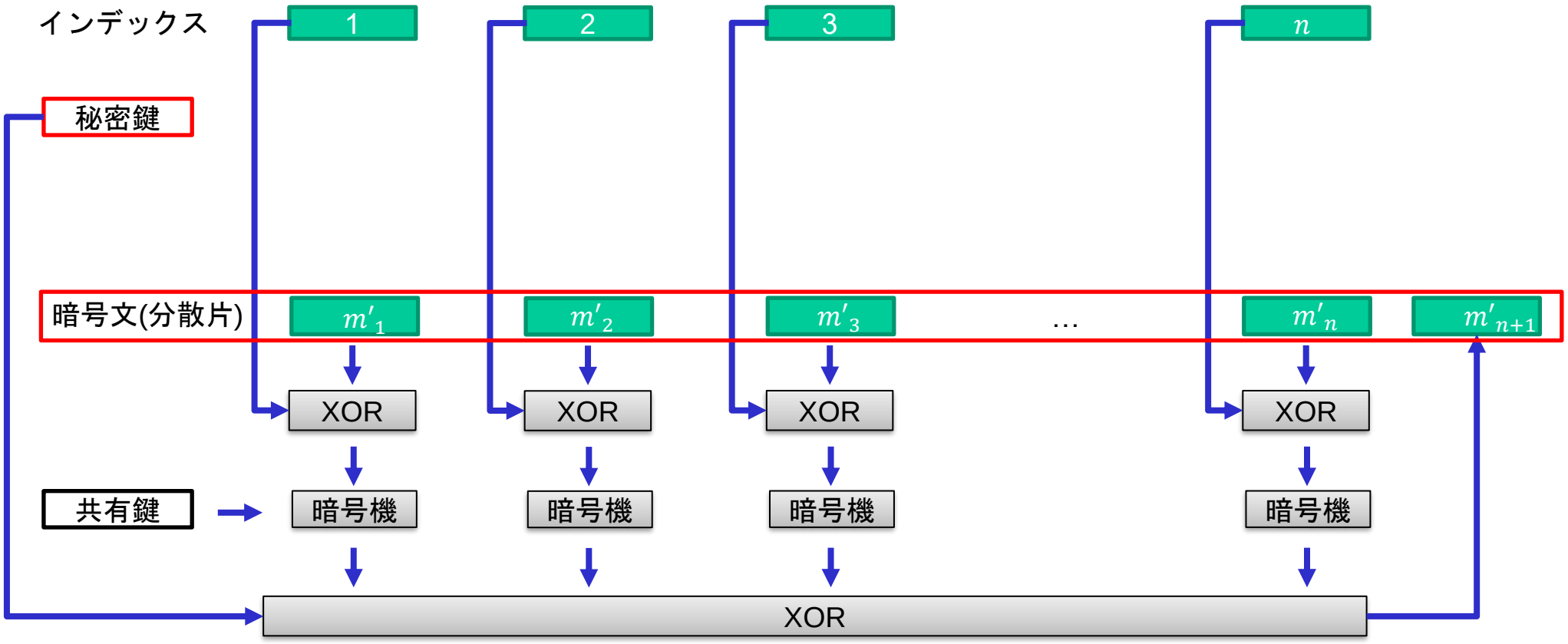
⇒　（平文に対する）分散片の作成が完了

秘密分散法
～AONT 分散化～



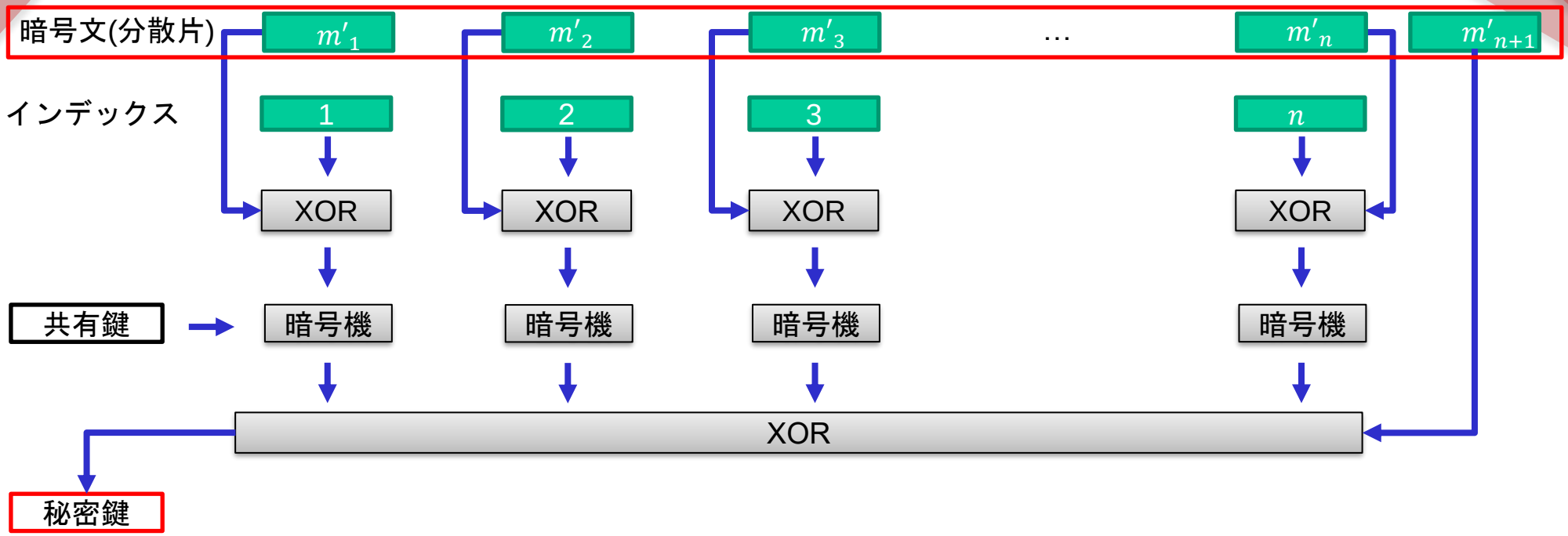
$m_n, m_2, \ldots, m_n$ とインデックスを XOR し、共有鍵で暗号化
秘密鍵と XOR をとり、 m_{n+1}とする（秘密鍵のための分散片）

秘密分散法
～AONT 復元～



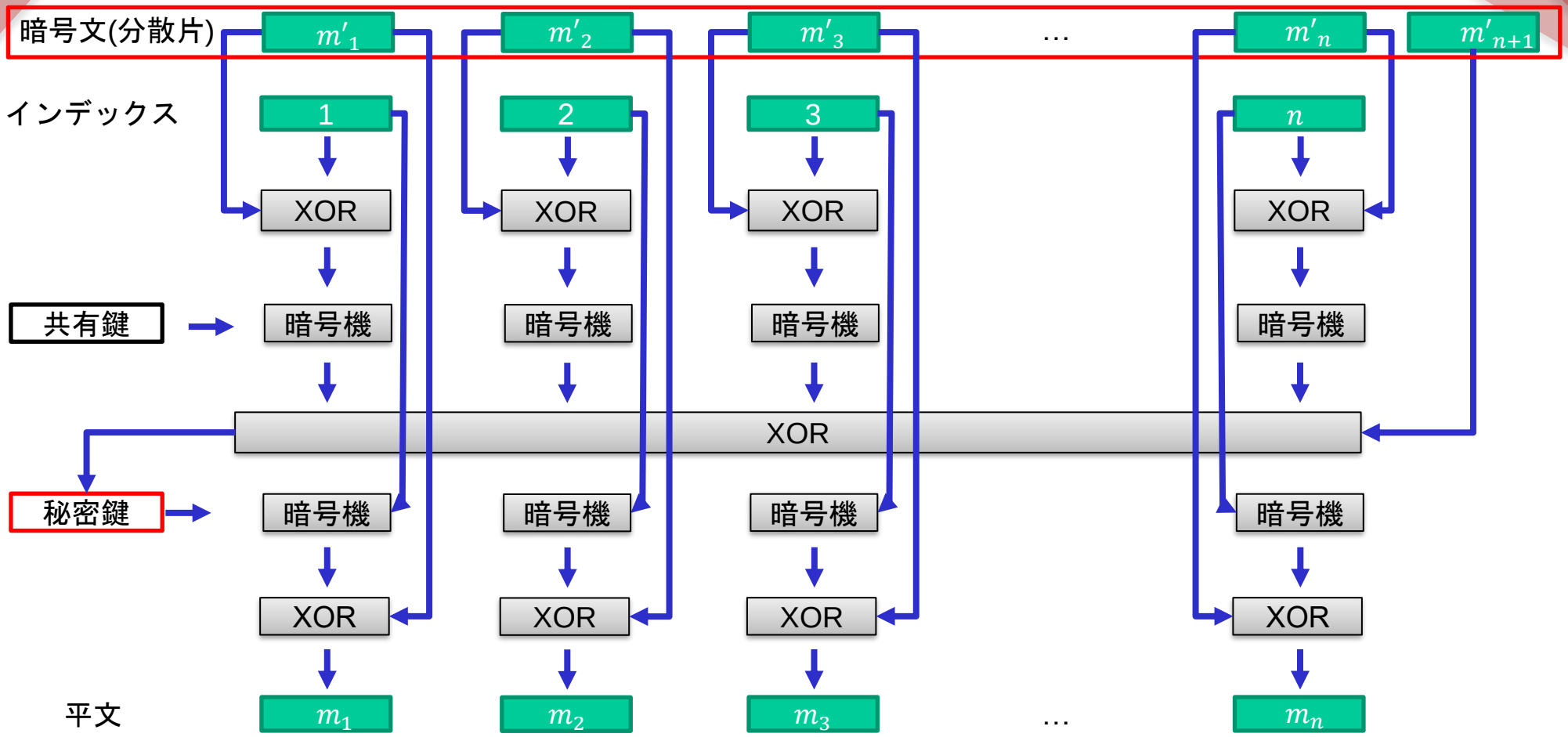
復元する側は、全ての分散片とそのインデックス、共有鍵を持っているのが前提

秘密分散法
～AONT 復元～



分散片 $m_n, m_2, \ldots, m_n$ とインデックスを XOR し、共有鍵で復号
さらに m_{n+1}と XOR をとり、秘密鍵を復元する

秘密分散法
～AONT 復元～



復元した秘密鍵を用いて、インデックス iを暗号器にかけ、
分散片 m_i と XOR し、（平文の）分散片m_i を復号する

秘密分散法
～AONT まとめ～

- **秘密鍵**の管理が不要（分散片に含まれる）
- 分散片を全て集めないと、復号側では**秘密鍵**の復元が不可能
  - 公開鍵暗号などでは秘密鍵が漏洩する場合、データの一部分が漏洩しても複合が可能
- 計算コストは低い(XOR と暗号処理だけ)

秘密分散法
～応用事例～

- PC や外部ストレージの保護（Zenmu Tech など）
- ライブラリ提供（リアルシス株式会社）
- データベース秘密分散保管（株式会社システムコンサルタント）

提言項目一覧

総論

- パンデミックを前提とした政策
- 昭和世代の責務
- デジタル田園都市国家構想
- DXの推進
- インターネットとその活用の見直しと法整備
- ネットワークとセキュリティのガイドライン改定
- データによる経済復興
- 健康を核としたデータガバナンス
- デジタルワーキングスタイル
- ライフラインを支える人々
- 新たな教育の在り方
- 新たな医療の在り方
- 防災分野の進化
- 新たなエンターテインメントの在り方
- 新たな担い手
- サイバーセキュリティの強化
- スーパーシティ/スマートシティの進化
- Society5.0の進化
- マイナンバー制度
- 行政分野

各論

- DXの推進
  - 社会全体のDX化の方向性
  - DX推進の仕組み
  - DXに向けた法整備
  - DXのための規制や制度の見直し
  - ネットワークとセキュリティのガイドライン改定
- 健康を核としたデータガバナンス
  - DTaaSとDFFT
  - セキュアな人の移動
- デジタルワーキングスタイル
  - 労働力のリバランシング
  - リモートワークの業務管理
  - 押印の見直し
  - 事務所登記とオフィス
  - リモートワークのネットワーク環境
  - オンライン名刺
- 新たな教育
  - 教育のDX化
  - オンライン教育の推進
- 新たな医療
  - オンライン医療の制度改革
  - 慢性疾患での「Pay for Value」化
  - 電子処方箋とHPKI
  - 医療分野でのデータ活用
  - 医療分野の技術開発
  - レセプトデータの所有権
  - オンライン診療の治験活用
  - 人とAIの協働
  - 感染症予防策
- 防災分野の進化
  - 高度広域防災プラットフォーム
  - 都市OSと防災
  - 自助/共助/公助
  - 分野間データ連携基盤
  - 災害時の医療データの活用
  - ベンチャ企業と大企業の連携
- エンターテインメントの進化
  - エンターテインメントの需要喚起
  - 新たなビジネスモデルとしてのコンテンツライブラリーの創出
  - 最新技術活用による新たな楽しみ方の提供
  - ライブハウス再開に向けた支援
  - デジタル発信充実に向けた支援
- 新たな担い手
  - スタートアップのための資金支援/投資
  - スタートアップのための税制
  - スタートアップのための規制緩和
  - スタートアップを活用したDXの社会実装
  - 雇用制度
- サイバーセキュリティの強化
  - 地域の中小企業に対する支援
  - 秘密分散、秘密/秘匿計算
  - ゼロトラスト
  - エンドポイントセキュリティ
  - 人間中心のスマートシティ
  - 2030年の未来都市
- Society5.0の進化
  - グローバル・サプライチェーンの見直し
  - トラストによる経済再興
  - 地方分散型デジタル基盤
  - 分野間データ連携基盤
- マイナンバー制度関連
  - 高まるマイナンバーカードへの関心と三密の発生
  - 地方公共団体情報システム機構の営業努力
  - 取得までのリードタイム短縮
  - 使えるのに使っていない業務
  - マイナンバーの提供・利用制限の緩和
  - マイナポータルを活用したサービスの拡充
  - 技術動向を見据えたカード使用の見直し
  - 公的個人認証サービスの電子証明書発行番号管理規制
  - マイナンバーカードの健康保険証利用範囲の拡大
  - 引越後の住所の開示
- 行政分野
  - 全体の方向性
    - DX組織(庁/省)の設置
    - 縦割りへの横串
    - 民間負担の軽減
    - 行政手続きのコンタクトレス化
  - 民間の負担軽減
    - 規制や慣行の見直し
    - 電子申請の効率化
    - データ連携/活用環境の整備
  - 官の効率化
    - 官庁の働き方
    - AIによる市民からの問い合わせの合理化
    - AIによる業務の効率化
    - デジタルウォレットの活用
    - LGWANの規制緩和
    - 感染状況の把握

©2020 自由民主党デジタル社会推進特別委員会 | Page No. 4

自民党デジタル社会推進特別委員会の
「デジタル・ニッポン2020」で秘密分散の推進を提言

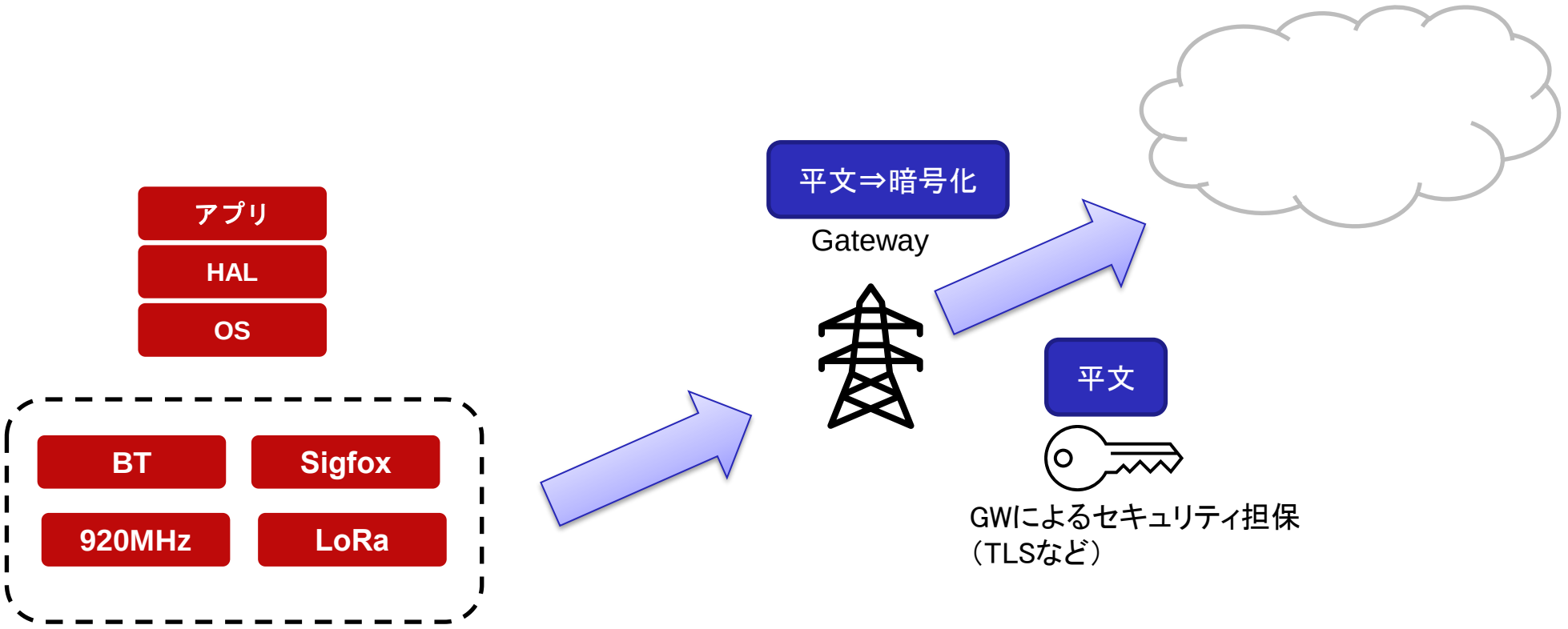
https://jimin.jp-east-2.storage.api.nifcloud.com/pdf/news/policy/200257_1.pdf

- サイバーセキュリティの強化
  - 地域の中小企業に対する支援
  - 秘密分散、秘密/秘匿計算
  - ゼロトラスト
  - エンドポイントセキュリティ

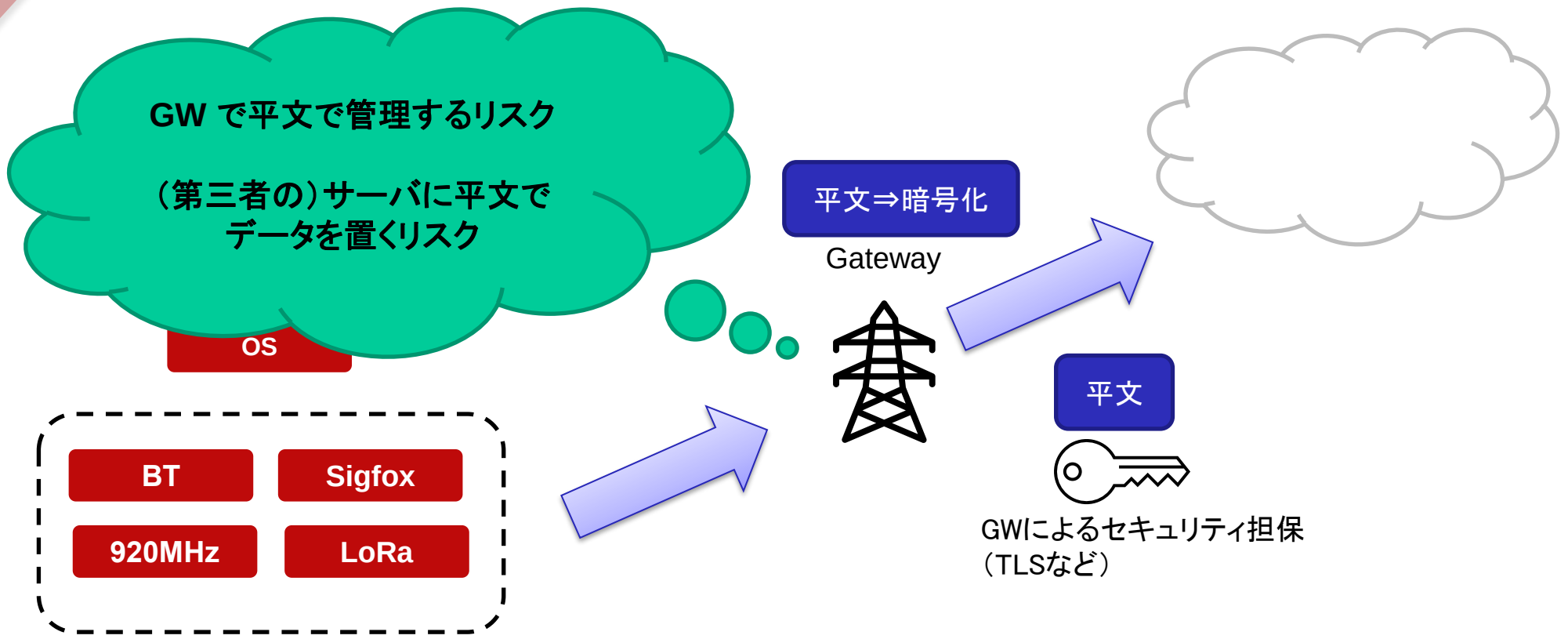
Agenda

- イントロダクション
- 組み込み向け軽量暗号
- 秘密分散法
- IoTA ～ 組み込み機器での実装例

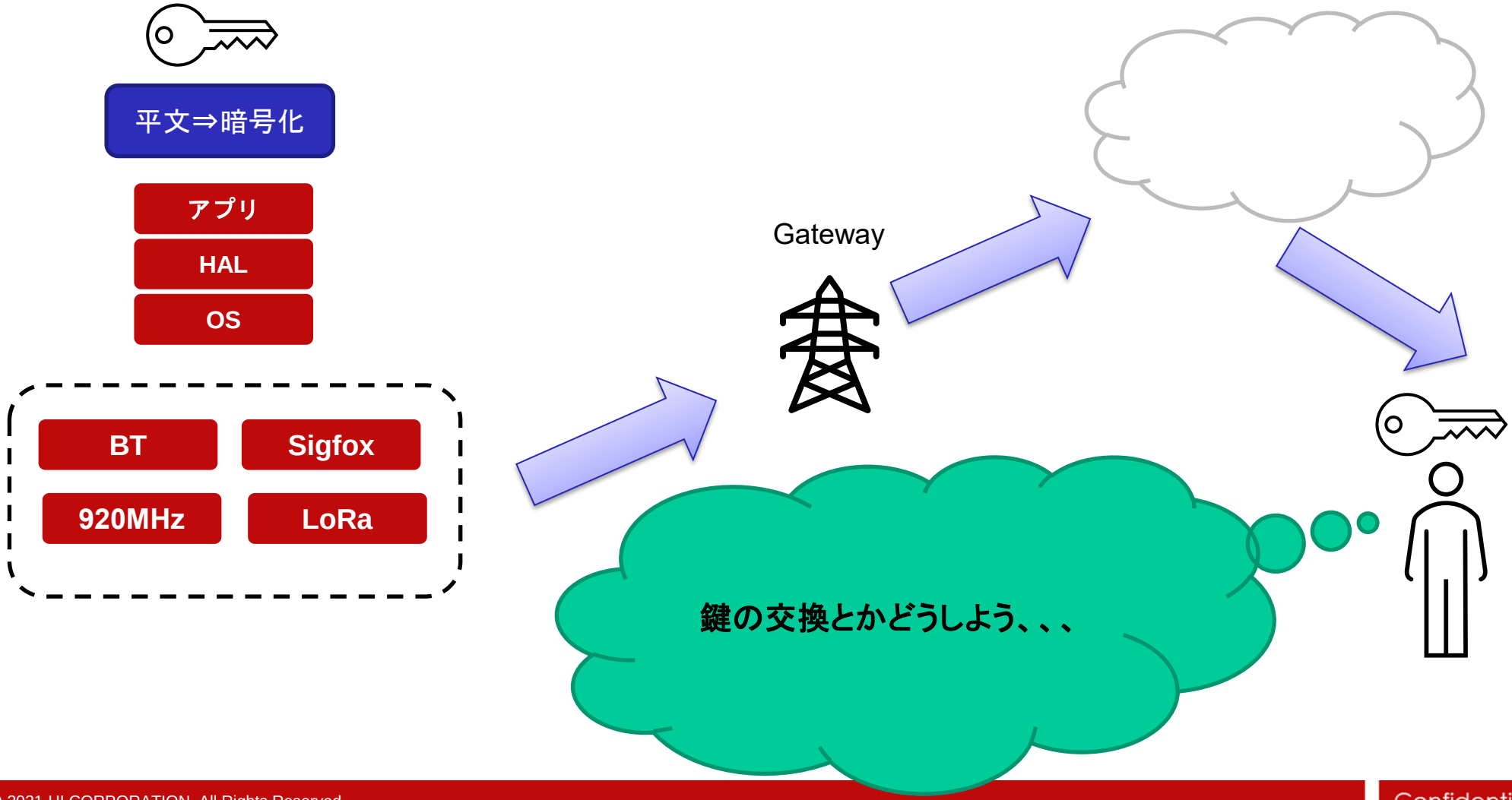
IoT デバイスにおけるセキュリティ担保



IoT デバイスにおけるセキュリティ担保



IoT デバイスにおけるセキュリティ担保



IoT デバイスにおけるセキュリティ担保

平文⇒暗号化

アプリ

HAL

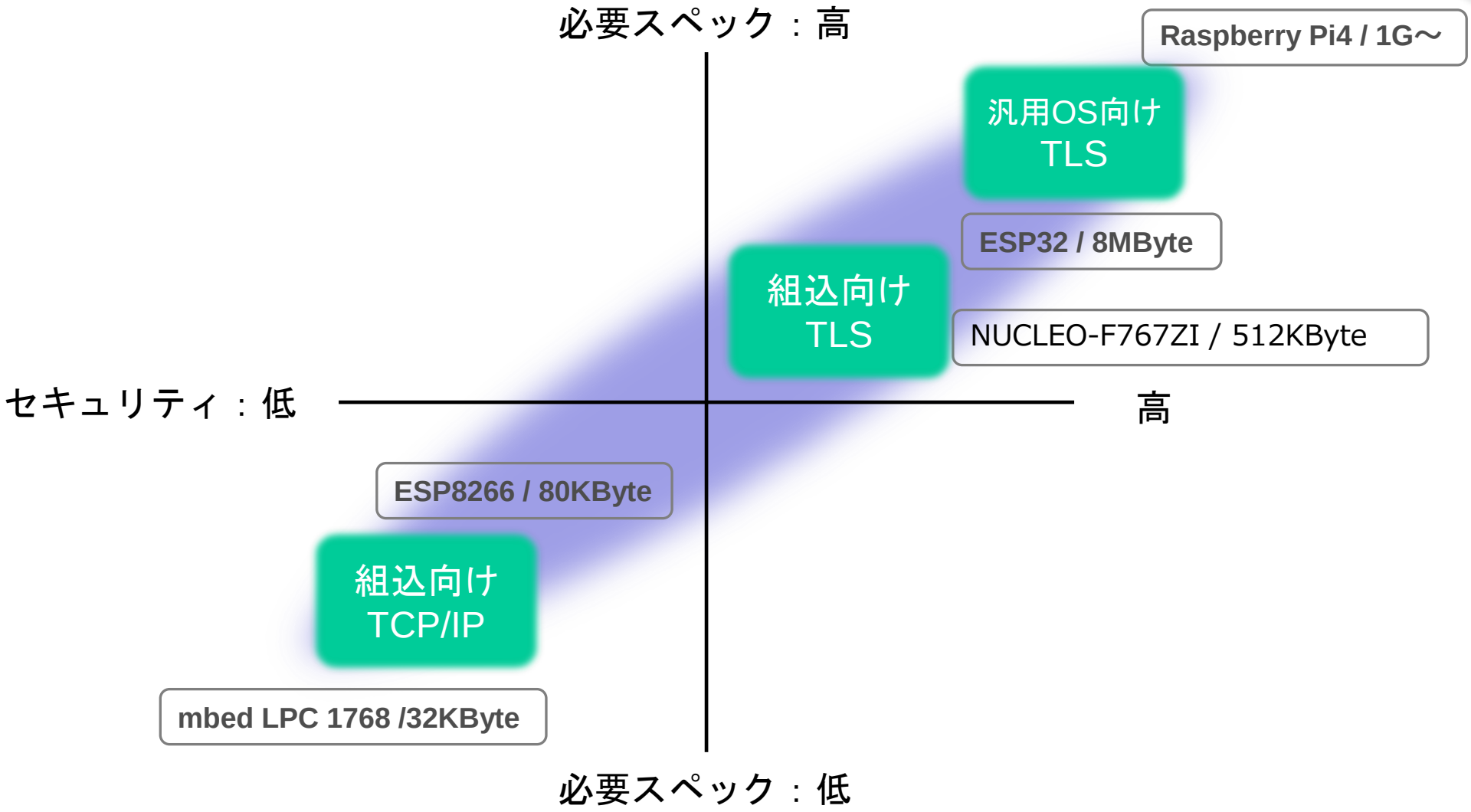
OS

2G/3G/4G　LTE-M

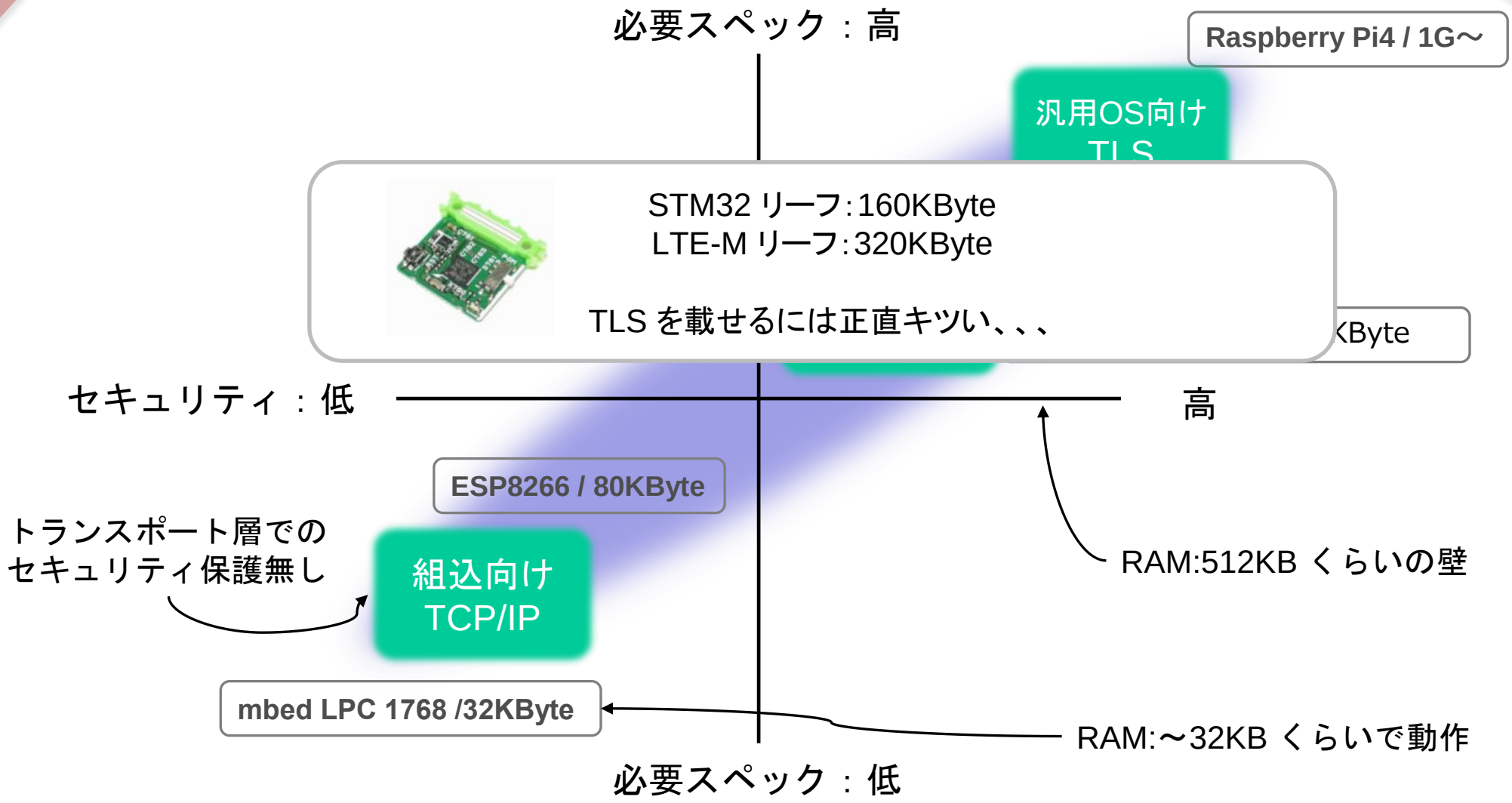
WiFi

TLS が載らない、、、

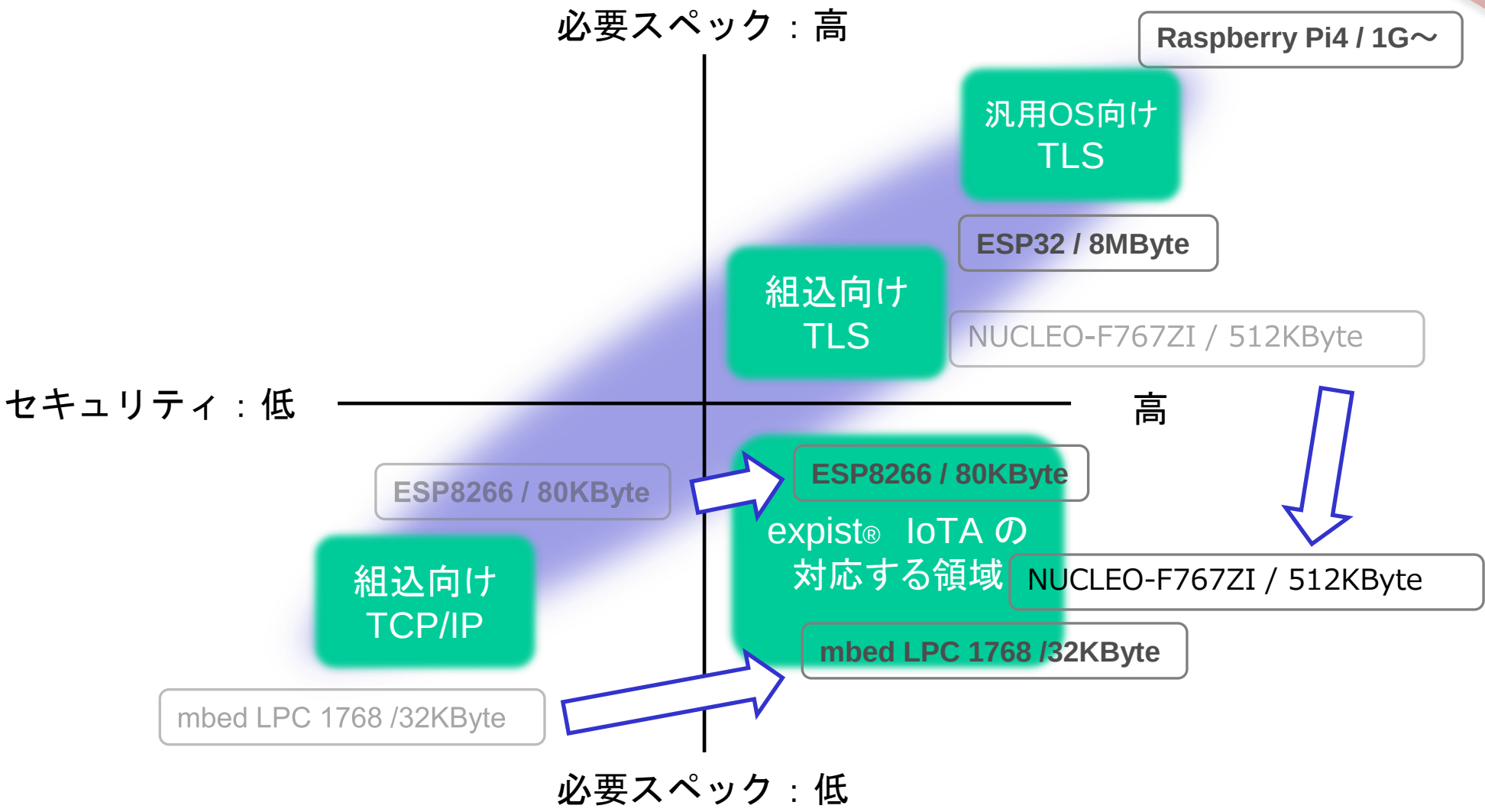
TCP/TLS(SSL) によるセキュリティ保護



TCP/TLS(SSL) によるセキュリティ保護



TCP/TLS(SSL) によるセキュリティ保護

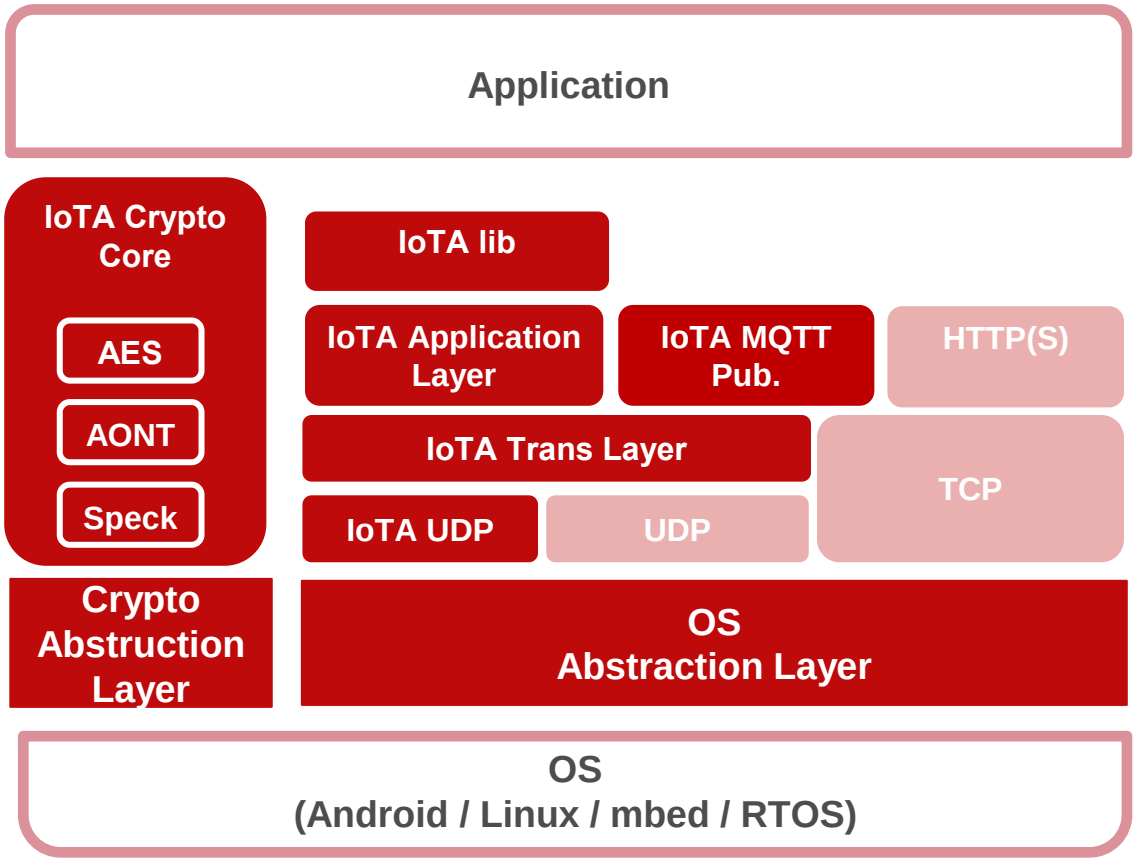


expist® IoTA

- UDP上で動作する独自プロトコル
- 軽量暗号サポート
- AONT による秘匿性向上

- 通信レジューム
- マルチセッションmTCP対応
- MQTT サポート
- パケット全体の暗号化

- Rust によるセキュア実装
- ISO 26262, 21434 対応



expist® IoTA

- エイチアイ開発の、省リソースで動作するサイバーセキュリティソリューション
  - 低スペックな SBC に対して、通信とセキュリティを導入
    - Cortex-M クラス～を想定
    - **ROM 64KByte / RAM 16KByte で動作**
  - LPWA を意識した軽量設計、暗号アルゴリズム
  - 移動中の通信であっても安定・堅牢

mbed LPC-1768

Raspberry-Pi Zero W

ESP8266

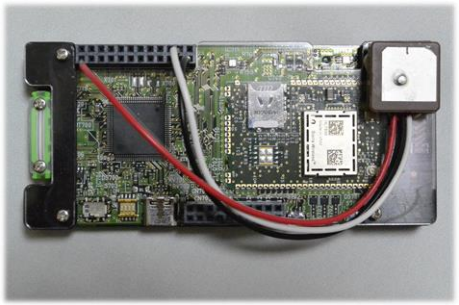
Leafony STM32

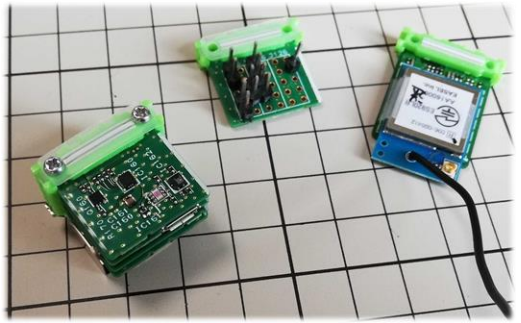
expist® IoTA

- 対応OS / プロセッサ（最低 ROM64KByte / RAM 16KByte）：
  - mbed OS (STM32、LPC 1768)
  - Linux （Raspberry Pi 4、Raspberry Pi Zero W、Intel Core シリーズ）
  - OS 非搭載（STM32、ESP32/ESP8266）

- 対応ドライバ
  - Linux Socket
  - lwip （汎用の組み込み向け TCP/IP プロトコルスタック）用ドライバと互換性のある UDP 層
  - ドライバレス（シリアル）

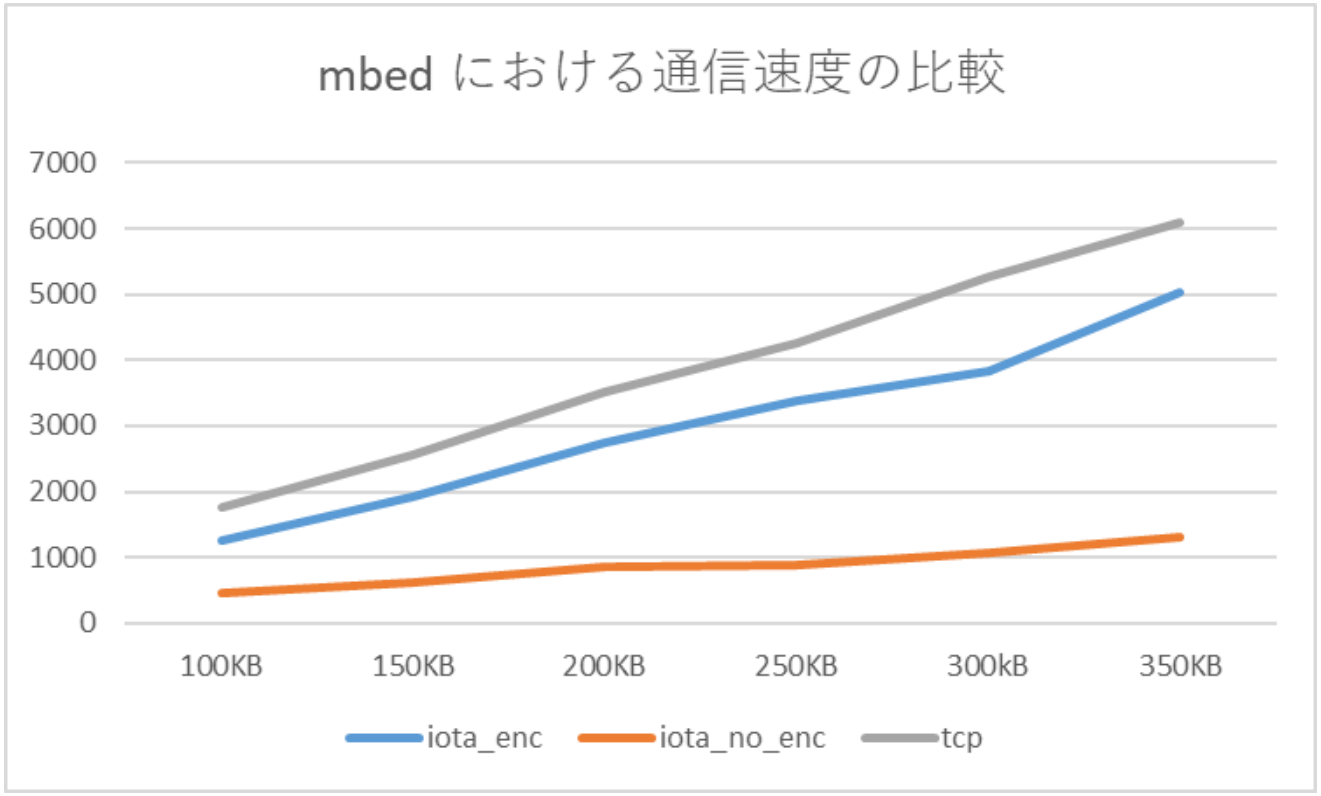
- 実績のあるサポート通信モジュール：
  - WiFi
  - Leafony LoRa リーフ
  - KDDI様 Leafony LTE-M Leaf
  - 佐鳥電機様 920MHz 通信モジュール
  - 佐鳥電機様 Sigfox 通信モジュール





expist® IoTA
～性能比較～

mbed NUCLEO-F767ZI Arm Cortex M7 216MHz における、IoTA と TCP の通信速度比較



iota_enc …
パケット全体を SPECK により暗号化

iota_no_enc …
パケット暗号化無し

tcp …
mbed OS に含まれるプロトコルスタック。TLS 無しの平文による通信

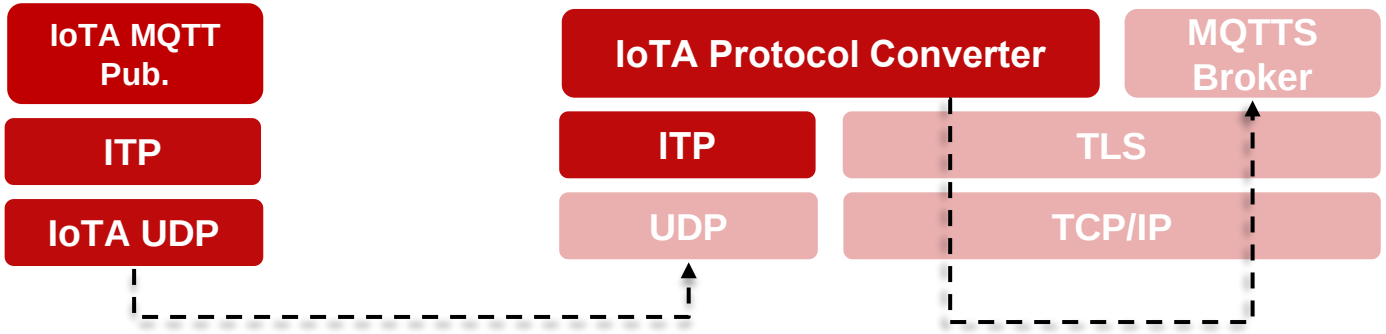
縦軸 ms,
横軸 転送データサイズ

⇒ 暗号化処理を入れても TCP に比べ IoTA が高速であることが確認出来る

expist® IoTA
～一般性の担保～

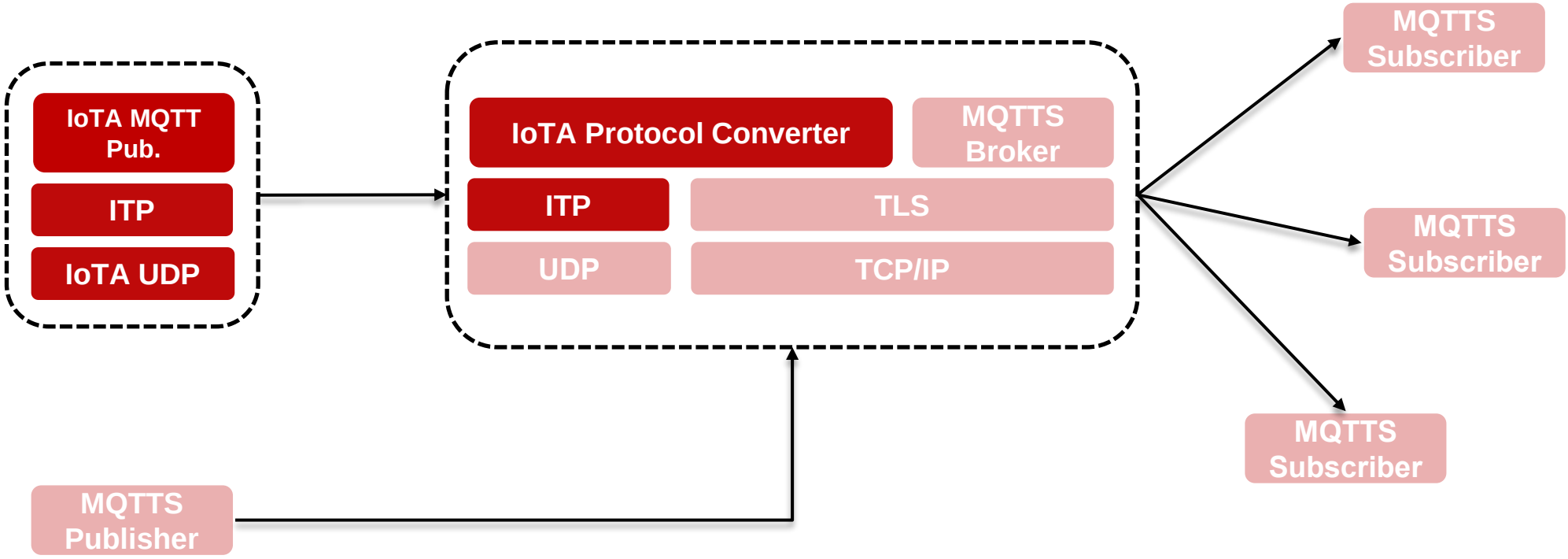
サーバ側は、IoTA　Protocol Converter により IoTA Transport Protocol = ITP を TCP/TLS に変換

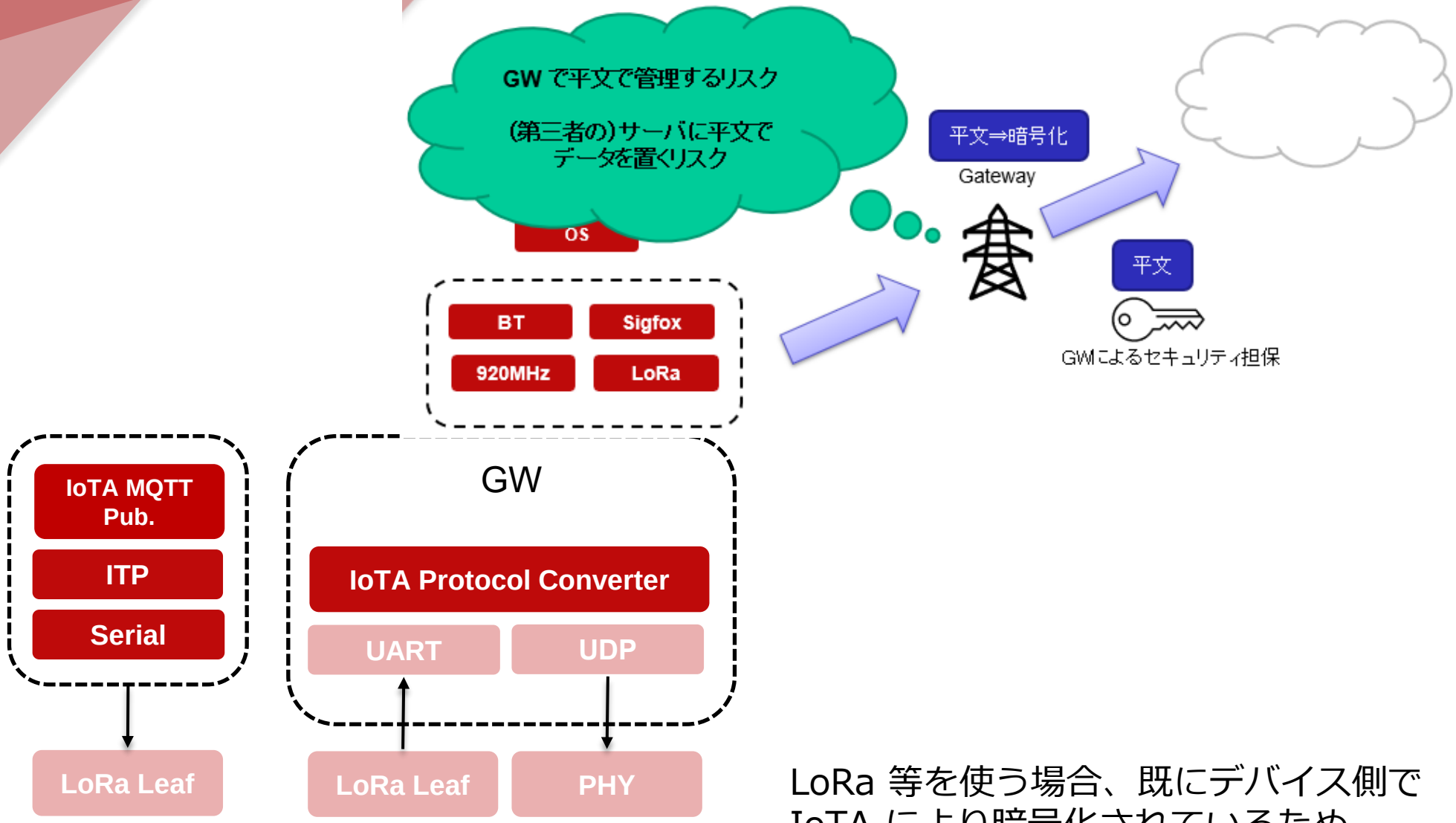
⇒　サーバ側アプリケーション資産を 100% 流用可能



expist® IoTA
～一般性の担保～

既存の MQTTS Publisher （＝リッチ OS ）に加えて、IoTA しか動作しない低スペックデバイスも、ネットワークに参加可能となる

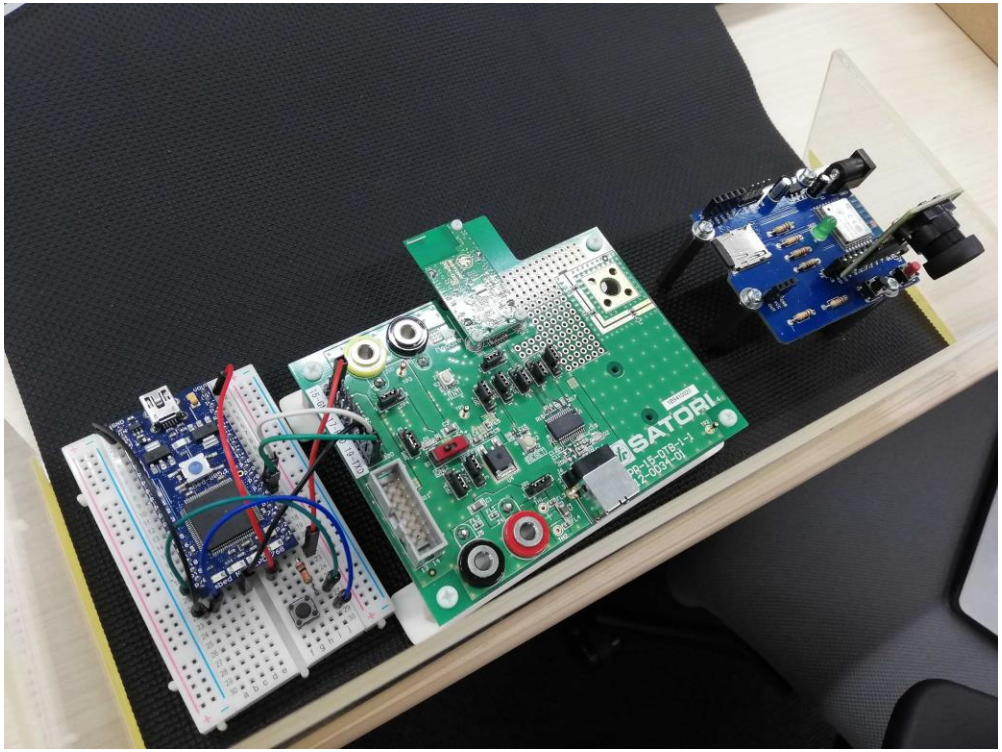




LoRa 等を使う場合、既にデバイス側で
IoTA により暗号化されているため、
GW において再暗号化などは不要

expist® IoTA
応用例

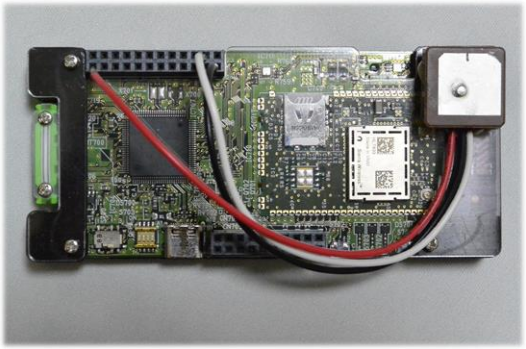
・LPC-1768 + 佐鳥電機様 920MHz 通信モジュールによるセンサーデータ送信
・ESP8266+カメラセンサによるセキュア画像配信

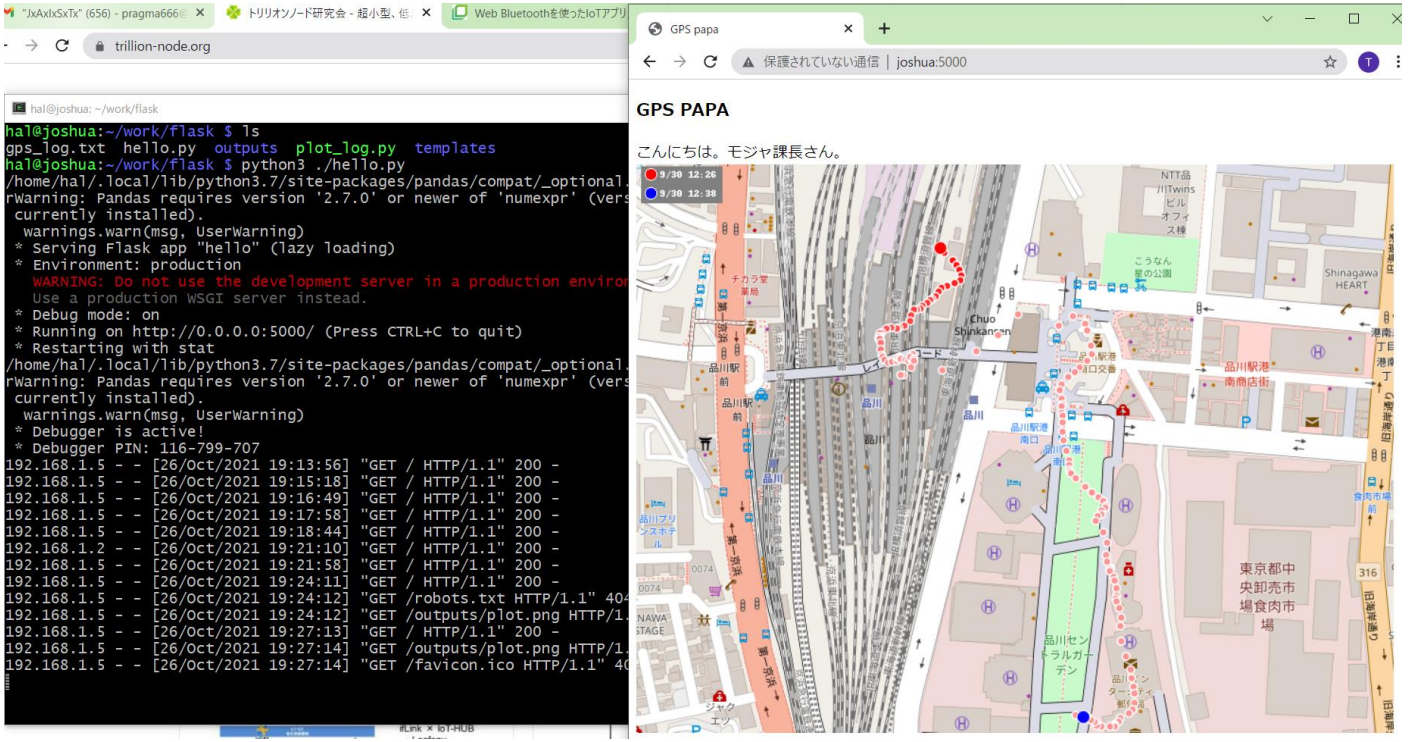


ET＆IoT展 @パシフィコ横浜/ JASA セキュリティ委員会ブース CA-14 で展示中

expist® IoTA 応用例

KDDI 様 Leafony LTE-M モジュールによる GPS 情報トラッキングシステム





ナノコン応用コンテスト「みまもりパパ」 / 12月9日にデモ・プレゼン予定

まとめ

IoT 機器へのセキュリティ対策のニーズが高まっている

組み込み機器へ暗号処理を導入する場合、SPECK が推し

情報漏洩に対して秘密分散法は堅牢性を持つ

これらの課題、特徴を取り入れた、エイチアイによるサイバーセキュリティソリューションの IoTA について紹介した

まとめ

内容に関するご質問、お問合せは以下までお願いします！
suzuki.takaharu@hicorp.co.jp