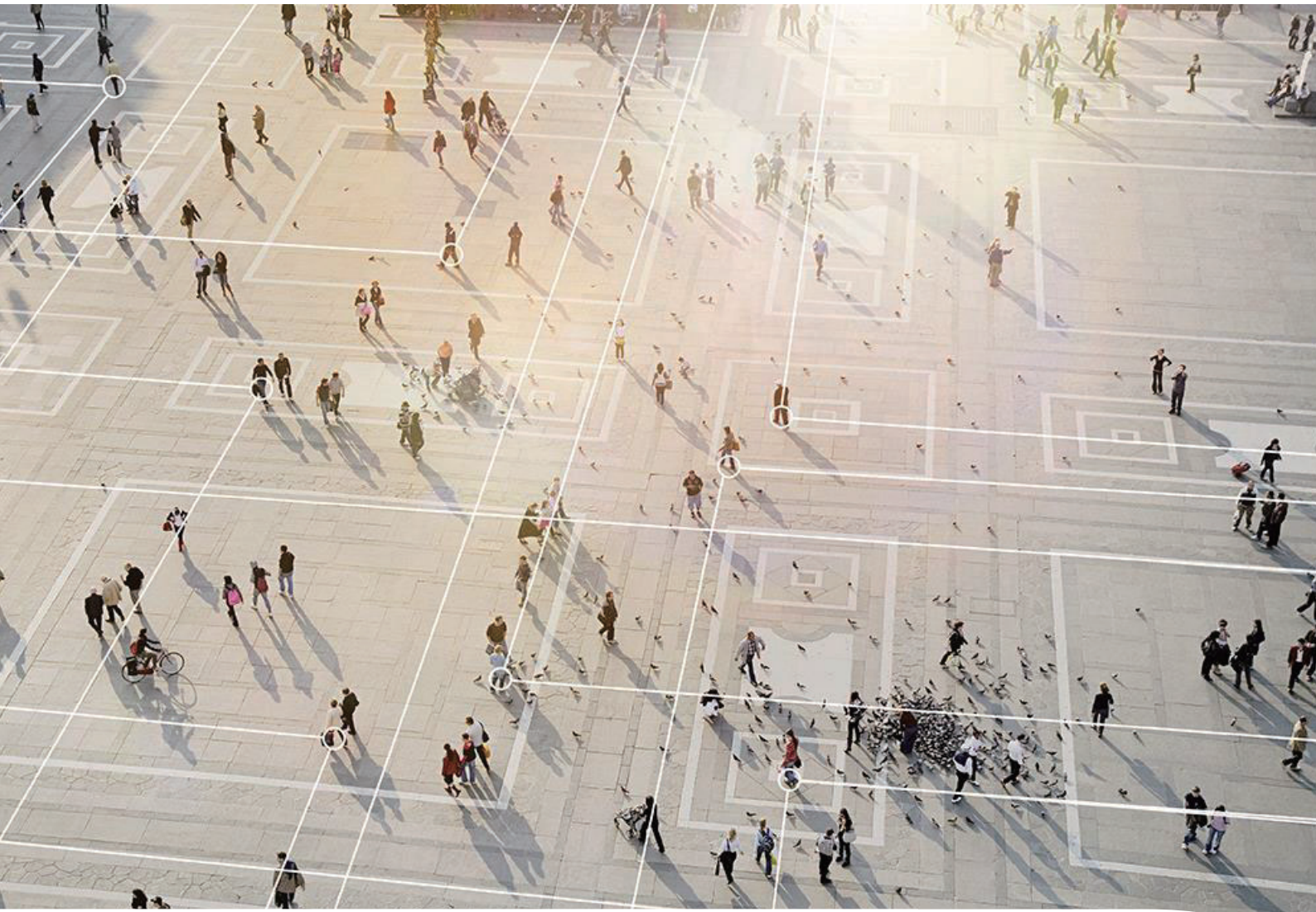
FUJITSU

FUJITSU Security Solution
脆弱性検証サービス

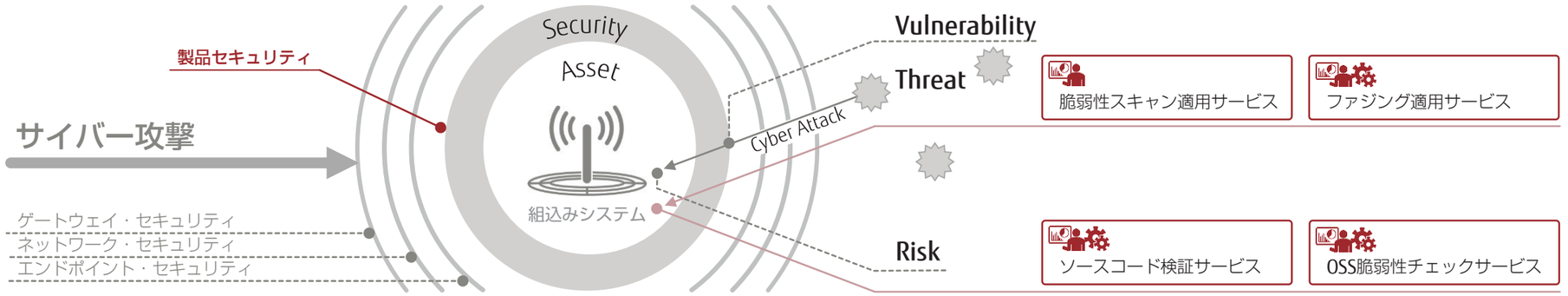


shaping tomorrow with you
社会とお客様の豊かな未来のために

増加するサイバー攻撃

サイバーセキュリティの必要性

IoTの普及・拡大でインターネットへ接続する組込みシステム（IoTデバイス）が急激に増加し、それに伴いサイバー攻撃の脅威・リスクが増大しています。実際にサイバー攻撃の半数以上は組込みシステム（IoTデバイス）が標的という調査結果もあり、組込みシステムのセキュリティは喫緊の課題です。近年「IoTセキュリティガイドライン」等の指針やセキュリティ標準規約の整備が進んでいますが、脆弱性対策に取組むには具体的な方策整備が必要です。弊社は長年培った組込みシステム等の開発・検証技術をベースとして、お客様のセキュアな組込みシステム開発をフルサポートします。



組込みシステム開発に必要な脆弱性対策

ソースコード検証サービス

要件定義 / 設計 / **実装** / テスト / 出荷・運用

解析結果（例：Buffer Overflow）

```
2586:  unsigned char *p = &s->s3->rrec.data[0], *pl;
2588:  unsigned int payload;
2589:  unsigned int padding = 16; /* Use minimum padding */
2592:  hbtype = *p++;
2593:  n2s(p, payload);
2594:  pl = p;
2601:  if (hbtype == TLS1_HB_REQUEST) {
2603:    unsigned char *buffer, *bp;
2610:    buffer = OPENSSL_malloc(1 + 2 + payload + padding);
2611:    bp = buffer;
2614:    *bp++ = TLS1_HB_RESPONSE;
2615:    s2n(payload, bp);
```

この引数は、攻撃者によって制御される可能性があります。汚染された可能性のある値が、適切な範囲の値であると仮定される可能性があります。

```
2616:    memcpy(bp, pl, payload);
```

参考：OpenSSL heartbeat

ソフトウェア開発の実装工程（プログラミング）では、コーディング・ルールに代表される「厳格な基準の適用」と品質確保のための「検証」が求められます。
ソースコード検証サービスは、開発スタイルに合わせた最適な静的解析ツールによる静的解析と、プロフェッショナルによる結果分析により、ソースコードの品質確保と実装工程のPDCAサイクル改善支援をサービスとして提供します。

静的解析ツール

対象ソフトウェアを実行せずソースコードを解析しバッファオーバーフローやメモリリーク等、脆弱性や信頼性に関わる欠陥を検出するツールです。
通常のレビューで見落とす可能性がある大規模なソースコード内の欠陥も網羅的な解析で検出します。また、CERT C等セキュア・コーディング・ルールの順守状況も検証可能です。

OSS脆弱性チェックサービス

要件定義 / 設計 / 実装 / **テスト** / 出荷・運用

解析結果（例：CVE 一覧）

```
:
CVE-2012-2686    2013/02/08 - CVSS v2 Base Score: 5.0
CVE-2014-0160    2014/04/07 - CVSS v2 Base Score: 5.0
```

OpenSSL の heartbeat 拡張に情報漏えいの脆弱性

[概要]

OpenSSL の heartbeat 拡張の実装には、情報漏えいの脆弱性が存在します。TLS や DTLS 通信において OpenSSL のコードを実行しているプロセスのメモリ内容が通信相手に漏えいする可能性があります。

```
CVE-2015-4000    2015/05/20 - CVSS v2 Base Score: 4.3
CVE-2016-0800    2015/05/20 - CVSS v2 Base Score: 4.3
```

ソフトウェア開発で増加しているOSS（オープンソースソフトウェア）の利用は、多くのメリットがある反面、脆弱性混入等のリスクが伴います。
OSS脆弱性チェックサービスは、ソフトウェアの設計から出荷まで幅広い工程で活用できるコンポジション解析ツールの導入・運用により、OSS利用時の脆弱性混入防止に向けた支援をサービスとして提供します。

コンポジション解析ツール

対象ソフトウェアのソースコードやバイナリを解析し、利用しているOSSに混入する「既知の脆弱性」やライセンス情報を可視化するツールです。
常に最新の脆弱性情報データベース（CVE等）と連動するため、OSS利用によって混入するソフトウェアの脆弱性について継続的に最新状況を確認することが可能です。

ファジング適用サービス

要件定義 / 設計 / 実装 / **テスト** / 出荷・運用

ソースデータ

```
GET index.html HTTP/1.1
Accept:*/*
Connection: Alive
```

ファズデータ

```
GET http://[?aAa::0] HTTP/1.1
Accept:*/*
Connection: Alive
```

データの一部をランダム変異して脆弱性を検証するデータを作成

応答結果判定：OKケース

```
Response data
HTTP/1.1 404 Not Found
```

応答結果判定：NGケース

```
Response data
time out
```

ゼロデイ攻撃（対策前の脆弱性を悪用した攻撃）に代表される「未知の脆弱性」を悪用した攻撃は、開発者が予め対策を取ることが極めて困難です。このような未知の脆弱性検出に有効とされる技術の一つが「ファジング」です。
ファジング適用サービスは、ファジングツールの導入・運用から検出内容の結果分析・再現調査等、効果的なファジングの実施支援をサービスとして提供します。

ファジングツール

対象システムにファズデータ（予測不可能なデータ）を送信することで、「未知の脆弱性」を検出するツールです。
HTTP・Bluetooth・CAN等の外部とのネットワークアクセスや、XML・オーディオファイル等の外部ファイル入力など、外部インターフェースを持つシステムに対する「未知の脆弱性」について検証可能です。

脆弱性スキャン適用サービス

要件定義 / 設計 / 実装 / **テスト** / 出荷・運用

エクスプロイトデータ(httpsパケット)

```
:
Content Type : Heartbeat(24)
Version      : TLS 1.1(0x0302)
Length       : 3
Heartbeat Message
  Type           : Request(1)
  Payload Length : 65535
  Payload(0bytes)
                 :
```

.. 18 03 02 00 03 01 ff ff ..

脆弱性を検証するデータを設定

応答結果判定：OKケース

```
Response data
error
```

応答結果判定：NGケース

```
Response data
over read
```

サイバー攻撃の99%以上は「既知の脆弱性」を悪用した攻撃であり対策が必要です。
脆弱性スキャン適用サービスは、脆弱性スキャナーを活用することでシステムのセキュリティに対する「既知の脆弱性」について検証します。また、セキュリティパッチの有無や提供状況や実在する攻撃を受けた時の危険度を可視化し、対策検討等の支援をサービスとして提供します。

脆弱性スキャナー

対象システムにエクスプロイト（サイバー攻撃プログラム）を送信することで、「既知の脆弱性」を検出するツールです。
初期パスワード使用による脆弱性や、マルウェアの混入等を検出します。また、ツールベンダーにより最新のエクスプロイトが定期的に更新されるため、最新の脆弱性情報に基づく「既知の脆弱性」について検証可能です。

「製品セキュリティ」関連サービス

開発工程別サービスメニューで総合的に対応

富士通グループでは、システム開発の上流から下流まで、各開発工程別に製品セキュリティ関連サービスをご用意しています。製品セキュリティの実現は品質と同様、上流工程から取り組むこと（セキュリティ・バイ・デザイン）が必要とされています。また、各工程で適切な対策を実施することで、リスクを低減することが可能です。

最適なサービスを柔軟に提供

サービス形態は、お客様に合わせてご対応します。
現状のセキュリティ状況を可視化・分析するレポーティングサービス、現場の課題を見つけだして解決を支援するコンサルティングサービス、ツールの販売や導入支援、教育プログラムの実施等、様々な形でご要望にお応えします。
一部のサービス、ツールはトライアルにも対応可能です。

提供サービス例

掲載のサービス、ツールは情報システム向けセキュリティ検証において多数の実績があります。

要件定義	設計	実装	テスト		出荷・運用
セキュリティ要件	セキュリティバイデザイン	静的検証	動的検証	妥当性確認	保守
基本方針検討・策定	脅威分析サービス	ソースコード検証サービス	脆弱性スキャン適用サービス	ペネトレーションテスト（第三者テスト）	
要件立案・分析	リスク分析サービス		ファジング適用サービス	OSS脆弱性チェックサービス	PSIRT構築
プロセス構築					
セキュリティ方針・要件を明確にし、対策の立案、計画、分析を実施することが、セキュアなシステム開発のスタートラインです。	上流工程で製品モデルを作成し、脅威分析から想定される「守るべき資産」と「リスク」を明確にします。その分析結果から製品セキュリティを決定します。	ソースコードに脆弱性を混入させないため、セキュア・コーディングガイドラインを定め、順守状況を確認します。人手によるレビューだけでなく、ツールの活用が品質向上・コスト削減に効果的です。	動作するシステムに対して、セキュリティに特化した検証を実施します。既知の脆弱性、未知の脆弱性を検出し、製品リリース前に脅威（その結果におけるリスク）の対策を実施します。	セキュリティの専門家が第三者の視点でセキュリティ・テストを実施します。OSSリスクの検証や侵入を試みるテストにより、運用を想定したシステム評価を実施します。	製品出荷後のセキュリティインシデントに対応する体制・ガイドラインを整備することで、緊急時に適切かつ迅速な対応が取れるように備えます。

- 富士通コンピュータテクノロジーズ提供サービス
- 富士通コンピュータテクノロジーズ販売・提供ツール
- 富士通コンピュータテクノロジーズおよび富士通・富士通グループ各社提供サービス（要相談）
- 富士通・富士通グループ各社提供サービス（要相談）

※本資料に記載されている内容については、予告なしに変更する場合がありますのでご了承ください。

お問い合わせ先
株式会社 富士通コンピュータテクノロジーズ
〒211-8588 神奈川県川崎市中原区上小田中4-1-1
http://www.fujitsu.com/jp/fct/

1511ka2