Appendix.　「電子証明書」と「ECC」の概説

■電子証明書（Certificate）とは

「X.509」は、「国際電気通信連合（International Telecommunication Union、ITU）」の標準規格の一つで、「Abstract Syntax Notation One（ASN.1）」記法によって公開鍵証明書の構造を定義します。基本的に、電子証明書は、第 1 階層の 3 項目から成るシーケンスで、署名されるべき電子証明書情報、署名アルゴリズム識別子、証明書の信頼性を検証する署名値、で構成されています。この構造は、以下の ASN.1 で表されます。

```
Certificate  ::=  SEQUENCE  {
     tbsCertificate       TBSCertificate,
     signatureAlgorithm   AlgorithmIdentifier,
     signatureValue       BIT STRING  }
```

電子証明書はそれ自体が、さらに複数の項目を含むコンポーネントで構成されるシーケンスです。

```
TBSCertificate  ::=  SEQUENCE  {
        version         [0]  EXPLICIT Version DEFAULT v1,
        serialNumber         CertificateSerialNumber,
        signature            AlgorithmIdentifier,
        issuer               Name,
        validity             Validity,
        subject              Name,
        subjectPublicKeyInfo SubjectPublicKeyInfo,
        issuerUniqueID  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
                             -- If present, version MUST be v2 or v3
        subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
                             -- If present, version MUST be v2 or v3
        extensions      [3]  EXPLICIT Extensions OPTIONAL
                             -- If present, version MUST be v3
```

ここで特に重要なのが「SubjectPublicKeyInfo」項目です。これは、公開鍵に使用するアルゴリズム情報を含むシーケンスで、その後に公開鍵情報が続きます。

```
SubjectPublicKeyInfo  ::=  SEQUENCE  {
     algorithm            AlgorithmIdentifier,
     subjectPublicKey     BIT STRING }
```

「AlgorithmIdentifier」構造体は、公開鍵と署名アルゴリズム両方の情報とパラメータを格納するために使用され、オブジェクト識別子（OID）と、OID で識別される特定のアルゴリズムに応じたパラメータで構成されます。

```
AlgorithmIdentifier  ::=  SEQUENCE  {
      algorithm               OBJECT IDENTIFIER,
      parameters              ANY DEFINED BY algorithm OPTIONAL  }
```

公開鍵のコンテキストにおいて、アルゴリズムのフィールドには例えば「rsaEncryption」のような多くの暗号化アルゴリズムの 1 つが記載されます。rsaEncryption の OID は 1.2.840.113549.1.1.1、dsa の OID は 1.2.840.10040.4.1、ecPublicKey の OID は 1.2.840.10045.2.1 です。OID が「ecPublicKey」のものに該当すれば、公開鍵は楕円曲線暗号処理に基づいていることを意味します。その場合、パラメータのフィールドは、RFC 3279 に定義されているように、「EcpkParameters」に対応するパラメータの 1 つに設定されます。

```
EcpkParameters ::= CHOICE {
   ecParameters  ECParameters,
   namedCurve    OBJECT IDENTIFIER,
   implicitlyCA  NULL }
```

言い換えると、楕円曲線は、曲線のパラメータを暗黙的に指定する、よく知られた「名前付き曲線」の 1 つに対応する OID を提供するか、あるいは「ecParameters」に曲線パラメータを明示することによって定義できます。問題の脆弱性は、攻撃者が名前付き曲線ではなく ecParameters を使用して細工した証明書を提示することにより発生します。しかし、なぜ発生するのかを説明するために、楕円曲線について概説します。

■楕円曲線（Elliptic Curves）とは

楕円曲線は、次の方程式で定義されます。

```
y^2 = x^3 + ax + b
```

楕円曲線暗号において、この方程式の解は、ガロア体とも呼ばれる有限体の範囲内で計算されます。有限体は、有限個の要素からなる体（Field）のことで、通常、素数 p あるいは素数のべき乗 p^n を位数としてすべての剰余

演算を実行することで作成され、GF（p^n）で表されます。与えられた楕円曲線上の点は、素体（Prime Field）が｛0,1,2、…、p-1｝の範囲の x 座標と y 座標で構成されます（つまり、累乗 n は 1）。集合内の元素の数は体の位数として知られており、楕円曲線の位数は曲線上のすべての点で構成されます。

ECC に使用される楕円曲線は、基点（ベースポイント、計算の開始点）を定義します。これは、曲線上で他の点を生成するために使用できる曲線上の特定の点です。有限体の位数の範囲内の整数で点に乗算することにより定義されます。名前付き曲線の場合は、係数 a および b、フィールド識別子（通常は素数 p）、および基点はすべて事前に定義されており、各曲線の公式標準に文書化されています。

しかし、電子証明書が明示的な「ecParameters」を定義する場合、以下の「ECParameters」の ASN.1 構造体に見られるように、曲線のすべてのパラメータが明示的に選択され証明書に表示されます。

```
ECParameters ::= SEQUENCE {
  version   ECPVer,          -- version is always 1
  fieldID   FieldID,         -- identifies the finite field over
                             -- which the curve is defined
  curve     Curve,           -- coefficients a and b of the
                             -- elliptic curve
  base      ECPoint,         -- specifies the base point P
                             -- on the elliptic curve
  order     INTEGER,         -- the order n of the base point
  cofactor  INTEGER OPTIONAL -- The integer h = #E(Fq)/n
  }
```

これらのパラメータを操作して、攻撃者が作成した鍵を使用して証明書を生成することが可能になり、攻撃者によって作成された公開鍵は既存の電子証明書の公開鍵と同一になります。これは通常、基点を変更し、他のすべての曲線パラメータは元の証明書が使用する名前付き曲線の事前に定義されたパラメータのままにしておくことで実行されます。

TREND MICRO ™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information. Our innovative solutions provide our customers with layered security for data centers, cloud workloads, networks, and endpoints.

At the heart of our leadership, Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights with the public, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on targeted attacks, artificial intelligence, Internet of Things (IoT), cybercriminals, and more. We continually work to anticipate the next wave of threats and deliver thought-provoking research that can shape strategic industry direction.

www.trendmicro.com