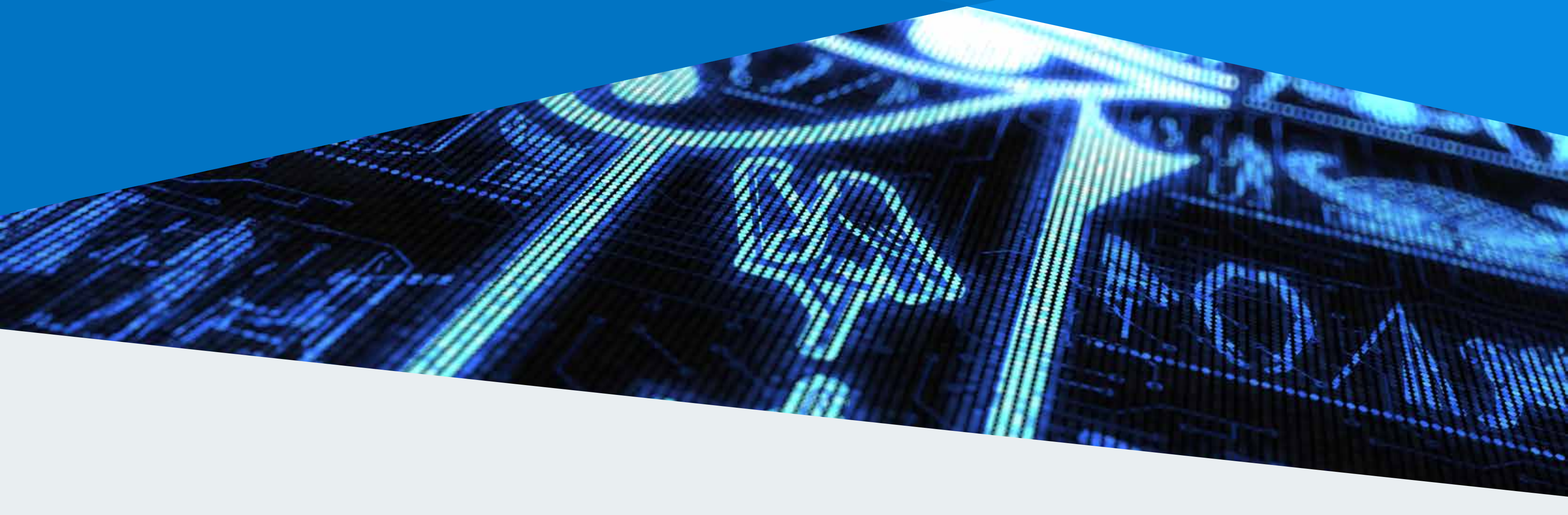
digicert®

コンピューティング時代の暗号化技術

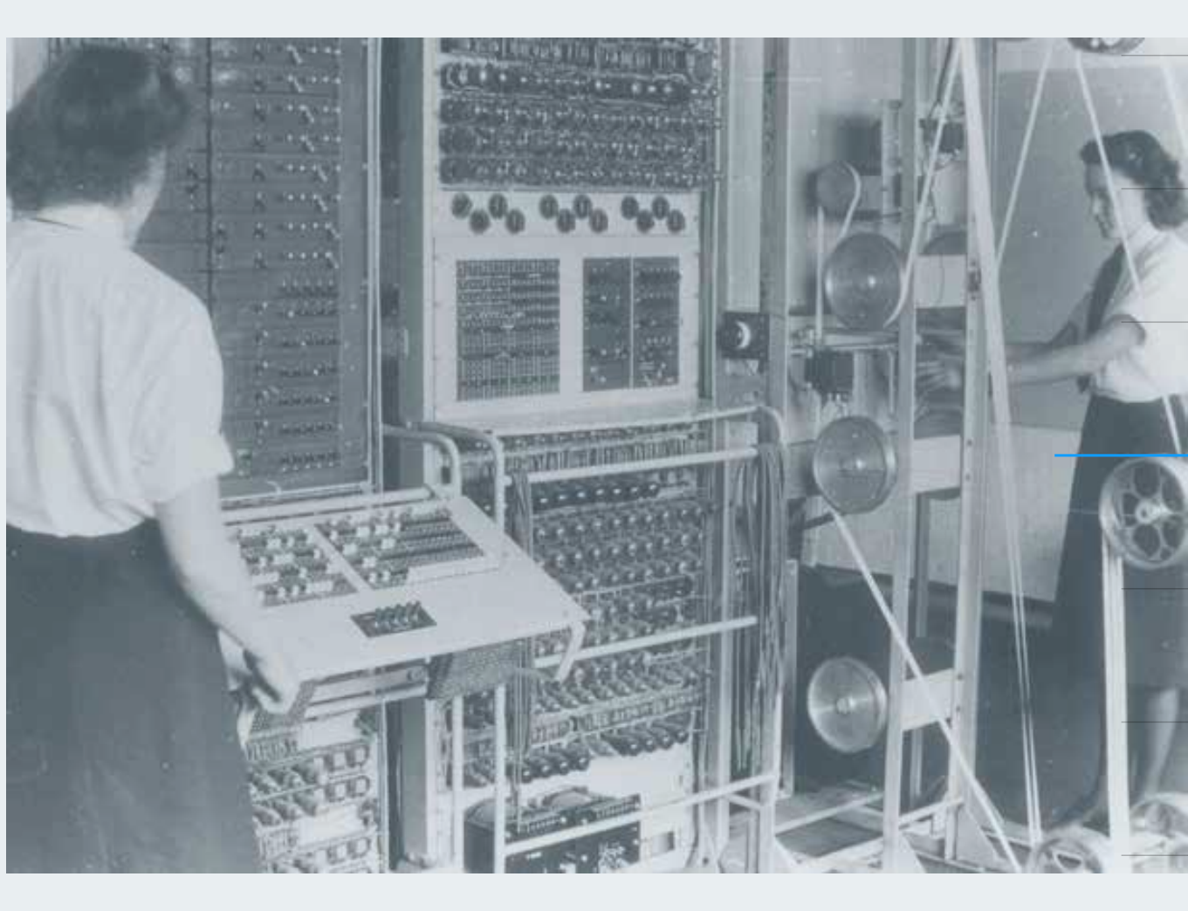


新たな暗号化のアルゴリズムが開発されると次にそれを解読するための手法が
生み出されます。この繰り返しが暗号化技術の歴史なのです。
このサイクルの次のフェーズに登場するのが量子暗号化技術です。
この技術では、暗号化された情報の受け取りに光子の振動角を利用します。

1974

諜報基地 ブレッチリー・パーク

ナチスが用いたエニグマ暗号機の暗号の解読にブレッチリー・パークの諜報基地がかかわった件で情報が公開されたときに、暗号解読においてコンピューターの果たす役割をはじめて一般の人々が意識するようになりました。



NIST

国立標準局（NBS）（のちに米国国立標準技術研究所（NIST）に改称）が承認したデータ暗号化標準（DES）の暗号方式は、その後、世界中で標準の方式になります。

1976

RSA®

公開鍵暗号方式を実現するためのアプリケーションとして初めて登場したのがRSA Cipherです。公開鍵暗号方式では、誰もがアクセスできる公開鍵を暗号化に用い、復号には、情報の受信者だけが知っている秘密鍵を使用します。

1994

DES鍵

DES鍵の鍵の組み合わせは2の56乗、すなわち約7000兆ありますが、現在では、コンピューティング能力の向上によって、この鍵の暗号も解読できるようになっています。

1996

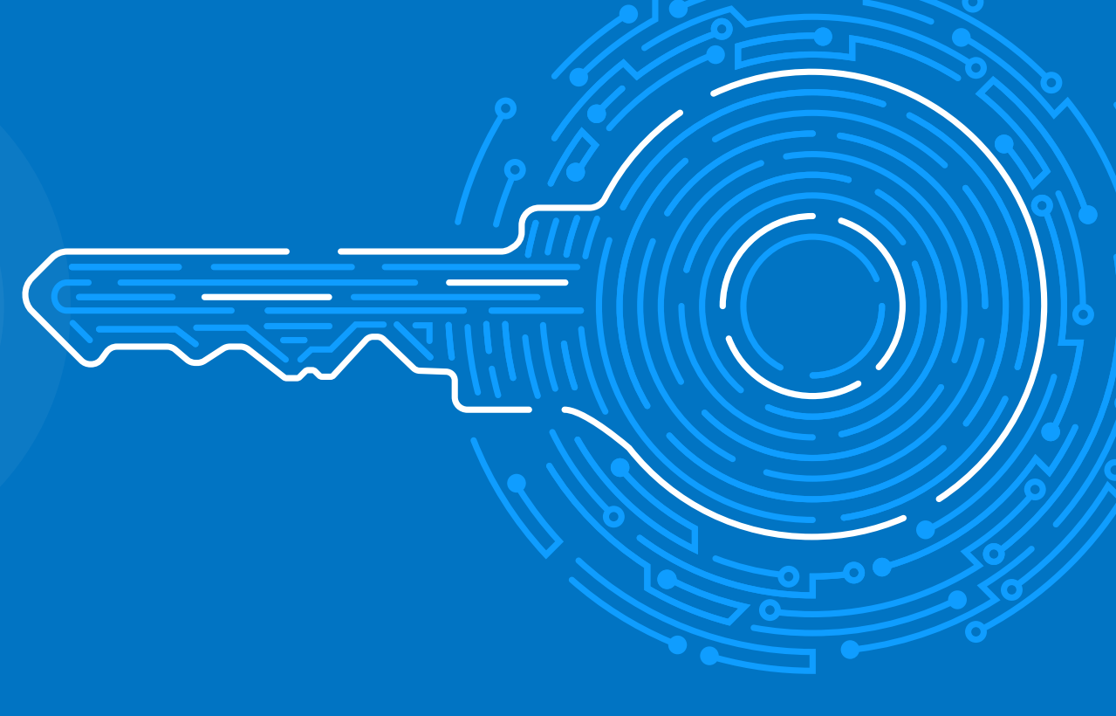
SSL

Netscapeは電子証明書を使ってサーバーの身元を明示的に確認するSSL（Secure Sockets Layer）バージョン3という仕組みを導入し、Netscape Navigatorというブラウザ製品に組み込みました。

1999

TLS

TLS（Transport Layer Security）1.0は当初、SSLバージョン3,0のアップグレードの位置付けにありました。



2005

ECC

米国国家安全保障局は、楕円曲線暗号（ECC）だけを使用してデジタル署名の生成と鍵の交換を行うSuite Bという方式を発表しています。

2014

2048ビット

NISTでは、1024ビットの証明書から2048ビットの証明書へ切り替えを行う期限を定めています。

```
-----BEGIN PUBLIC KEY-----
MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQK
ZWeLqiRZ7i7Ut0iU2W4N7IxgcT1RAu7mHJpTcgiMzm
TLSERu4cZv9LNS6bmo/c59AkeN2A86EfHx9+v0QaV
+pnIpxA9OWXTZs8XQzlmNhOIWTx9c2xjRp4MNjkud
AhHfEXabA5dawoRIzWwkjDTJnyoz8tx1WAPCPJiLdz
yg5KjnXgLFxcMmvw5FAYe0qBTkKXPO19dplos5Zwp
AgMBAAE=
-----END PUBLIC KEY-----
```

2019

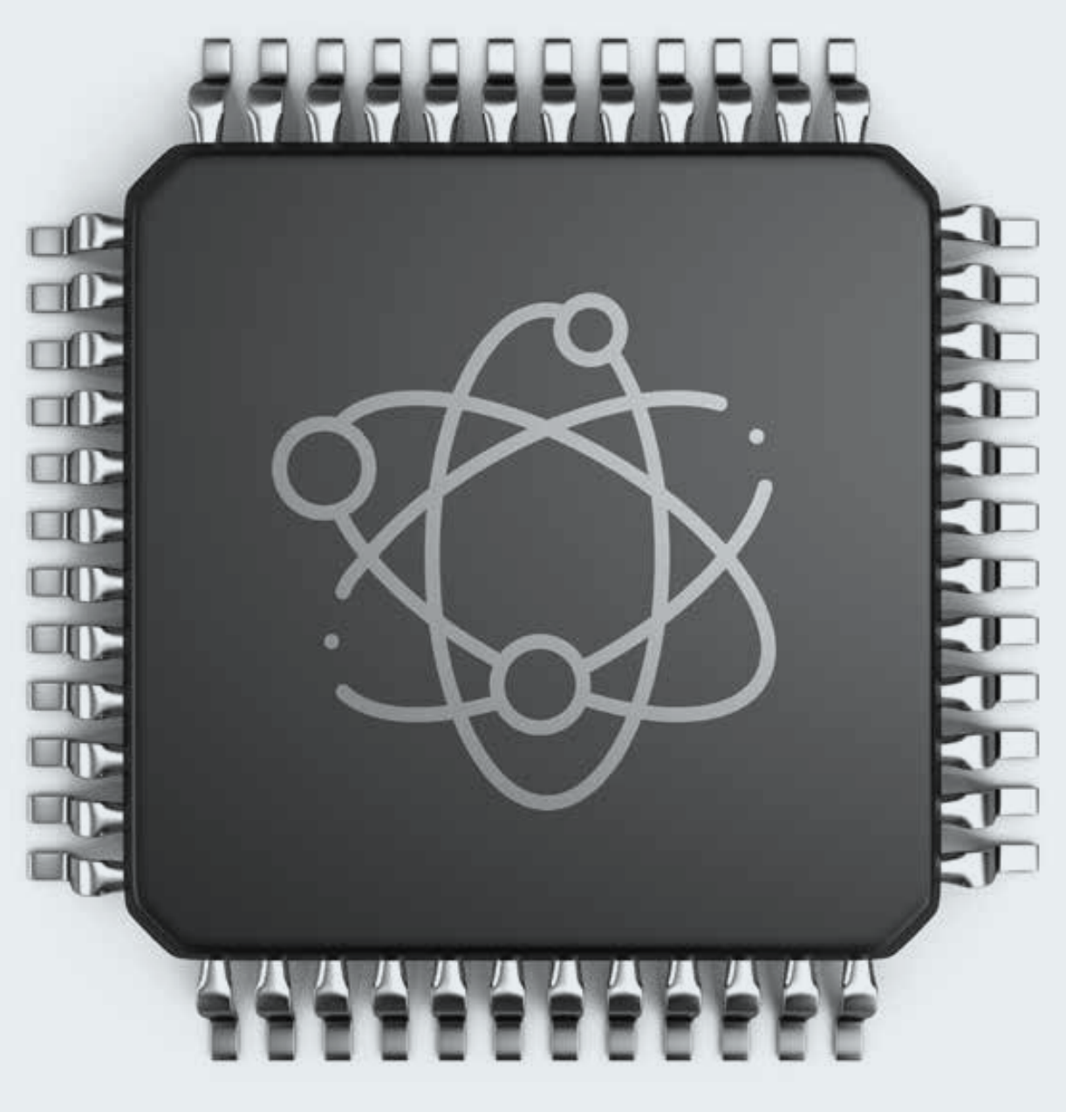
digicert®

旧来のコンピューティングテクノロジーを利用した場合、2048ビットのRSA鍵を解読するには数千兆年がかかるとDigiCertでは見込んでおり、この内容は、National Academyのレポートで確認できます。

2029

量子コンピューター

NISTの見通しによれば、量子コンピューターが同じ2048ビットの鍵を数か月で解読する日が今後10年以内に訪れると言います。これは、量子暗号化技術の時代の始まりを正式に告げる出来事になるでしょう。



digicert®

量子コンピューティングの時代に飛躍する

量子コンピューティングにより、RSAやECCといった暗号標準は崩壊します。
それが起こるのは間違いありません。問題はそれがいつ起きるかです。
この状況で先手を打つために、弊社のポスト量子暗号化（PQC）ツールキットを是非ご活用ください。

DigiCert.com/PostQuantum