コントロールドイツとトルコでは、彼らは特に悲惨なシーンを見ていた。  
 核兵器とコックピット内の外国人パイロットを搭載した迅速な対応の警告飛行機。  
米国の唯一の証拠  
ドイツの飛行場の歩哨がどのように核兵器の管理を維持するつもりであるかを尋ねられたとき、パイロットは突然スクランブルすることを決定しなければなりません（個人的な気まぐれによるか、またはアメリカを迂回するドイツ軍の命令による）。  
、歩哨はパイロットを撃つと答えた。アグニューは爆弾を撃つように彼に指示した。  
15.1はじめに  
核兵器管理は国際外交の中心です。北朝鮮は現在爆弾を抱えていますが、南アフリカとリビアはそれをあきらめるように説得されましたが、イランのプログラムは（外交的およびサイバー的手段によって）停止されました  
驚くべき量の核セキュリティのノウハウが発表されました。  
多くの国が核兵器を生産することができますが、しないことを決定しました（日本、オーストラリア、スイス、...）  
核不拡散の本当の力の多くは文化的であり、外交と、非核国家の手に渡った敗北に直面しているときでさえ、1945年以来これらの兵器の使用を予見していた核保有国の拘束によって構築されてきました。  
。  
したがって、政府間だけでなく、ますます懐疑的な国民からも国際的な信頼を呼び起こすような方法で、物事を守らなければなりません1。  
米国エネルギー省の武器研究所-サンディア、ローレンスリバモア、ロスアラモス-は、核兵器と核物質をできる限り安全にするために2世代にわたって取り組んできました。  
保護対象のデバイスに光ファイバーを巻き付け、干渉効果を使用して1ミクロン未満の長さの変化を検出するトリックも、それらの1つです。それは、武器庫の弾頭とループに間違いなくループするように設計されていますそれらのいずれかが移動された場合。  
たとえば、虹彩認証は、個人の生体認証で知られている最も正確なシステムで、現在はインドのアーダーアイデンティティシステムで使用されています。プルトニウムストアへの入店を制御するために、米国エネルギー省の資金を使用して開発されました。改ざん防止および改ざん検知技術の専門知識の元は、盗まれた武器や制御装置の乱用を防止するために最初に進化しました。  
2003年3月のイラク侵攻。その原因はイラクが大量破壊兵器を所有していたとの主張だった。 2。  
パキスタンの核計画の上級科学者であるアブドゥル・カディール・カーンが、シリア、リビア、イラン、北朝鮮を含む他の国々が武器技術を手に入れ、彼のネットワークを解体するのを助けた2004年の開示。 4。  
5。  
すべての努力が成功したわけではありませんが、明白な例は、北朝鮮です。1994年に米国との協定に署名し、石油輸送と引き換えに兵器開発を停止し、民間原子力の開発を支援しました。  
この歴史により、トランプ政権が2018年にイランとの合意を放棄したことによる長期的な影響の可能性を多くの人々が理解しています（イランは同意していましたが）。  
そして、2019年のロシアとの中距離核兵器条約の放棄もありました（ロシアの不正行為の結果であったとしても）  
核規制は、弾頭とその建設に必要な核分裂性物質以外にも適用されます。  
そのため、2007年にGAOの調査員は偽の会社を設立し、核規制委員会から同位体の購入を許可する免許を取得しました。  
テロへの恐怖のおかげで、核物質の規制は厳しくなり、経済により広がっています。  
たとえば、発生させたくない特定のアクションの確率が人為的エラーによって発生する確率が10分の1である場合、5人の異なる人に確認してもらうことで、確率を1分の1に減らすことができます。 100,000。  
しかし、2007年10月、ノースダコタ州のマイノット空軍基地からルイジアナ州のバークスデールまで巡航ミサイルを運ぶ飛行機に、生きた弾頭で武装した6つのミサイルが誤って搭載された後、6つの米国水素爆弾が36時間行方不明になった。、ミサイルを移動する前に検査が完了するのを待っている地上の乗務員によって（彼らはしなかった）  
、運転手がコントロールセンターに識別番号を呼び出すことによって（そこに誰もチェックする気になりませんでした）  
。  
これは、共有制御の制限の1つを示しています。  
実際、USAF事件では、飛行士が公式手順を独自の「非公式」スケジュールに置き換えたことが判明しました。  
 この章では、原子力安全環境と、アプリケーションを発見する（または脅威をもたらす）可能性があるいくつかのトリックについて説明します  
それは公共の情報源から集められたものですが、それでも、役立つ教訓が得られます。  
15.2指揮統制の進化  
その安全性はやや即興でした。  
しかし、重荷のあるB-29の多くは、彼らが使用していた基地であるテニアンからの離陸時に墜落しました。  
そのため、彼は襲撃の前日、プライマーの取り外しと再取り付け（パン1丁分の火薬代）を練習していたので、離陸後に取り付けることができました。  
それは進化の過程でした。  
コンビネーションロックへの移行がありました。パイロットは、離陸後に6桁のコードをワイヤードシールのふたが付いた特別なキーパッドに入力して爆弾を準備しました。  
しかし、1950年代の技術的制御と手続き的制御はどちらも原始的なものでした。  
15.2.1ケネディ覚書  
ソビエトのB-59はフォックストロット級のディーゼル電気潜水艦で、1962年10月27日に空母USSランドルフと11隻の駆逐艦からなる米国戦闘グループが近くに爆撃を仕掛け始めました。  
しかし、これは船上の3人の上級将校が同意した場合にのみ可能であり、幸運にも彼らの1人であるVasily Arkhipovが拒否した。  
これは、世界の戦争が偶然にアメリカの政策立案者に顕著になるリスクをもたらし、ケネディ大統領は彼の科学顧問ジェローム・ヴィースナーに調査を命じました。  
これらの武器はトークンの米国保管軍によって保護されていたため、危機の際に武器を押収できなかったという物理的な理由はありませんでした。  
ケネディの反応は国家安全保障行動メモでした。  
これにより、アメリカの7,000個の核兵器がNATOコマンドに分散され、米国または同盟軍の管理下にあるかどうかに関係なく、技術的な手段を使用して米国の積極的な管理下に置かれるように命じられました。  
 ウィスナーのリストのトップに実際にあった。  
基本的な原則は、武器が発動する前に環境のユニークな側面を感知しなければならないということでした。  
1つの例外がありました：原子爆弾の爆弾。  
偶発的または悪意のある爆発を防止するための独自の環境センサーの範囲はないようです。  
主なエンジニアリング問題はメンテナンスでした。  
したがって、すべての武器で同じコードを使用することは受け入れられませんでした。  
ケネディのメモに続いて、すべての核爆弾はコードロックを使用して保護されるべきであり、大統領または彼の後継者だけが与えることができる「ユニバーサルロック解除」アクションメッセージがあるべきであると提案されました。  
問題は、教義が大規模な報復から「測定された対応」に変わった1960年代と1970年代に悪化しました。  
。  
  
深い質問は、原子力安全システムとコマンドシステムが実施すべきセキュリティポリシーでした。  
弾頭を爆発させるには、3つの条件を満たす必要があります。  
。  
（原子爆弾では、この要件は特別なコンテナを使用することで置き換えられます。）  
初期のシステムでは、「認証」は4桁の認証コードをデバイスに入力することを意味していました。  
航空機は通常、6桁の武装または「使用制御」コードを使用します。  
実装が何であれ、固有のシグナルがなければなりません。 6桁のコードから導出された22ビットは、ユーザビリティから偶発的な武装のリスクを最小限に抑えることまでの多くの要因の間の適切なトレードオフであると考えられています[1349]。  
15.3無条件に安全な認証  
第5章「暗号化」で説明したように、これらは電信送金を保護するために発明されたテストキーと概念が似ています。キー付きの変換がメッセージに適用され、短い認証コードが生成されることも知られています。オーセンティケーターまたはタグとして。つまり、機密性のためにワンタイムパッドが行うことを認証のために行います。  
 または、既存の有効なメッセージを変更して、別のメッセージ（置換）を取得する  
第5章で説明したGCM動作モードでは、これらは2128に等しく設定されていますが、これは必ずしもそうである必要はありません。  
司令官が、000から999までの3桁の数字として命令がエンコードされる下位の認証スキームに同意したとします。  
これらの1つは偶数としてエンコードされ、もう1つは奇数によってエンコードされます。これは秘密鍵の一部になります。  
キーは次のとおりであると想定します。•「ロシアを攻撃」は偶数にコード化し、「中国を攻撃」は奇数にコード化します。•本物のメッセージは、337で除算すると、残りが12になります。  
 「攻撃中国」は「349」です。  
ただし、有効なメッセージが表示されたら（「Attack Russia」の場合は「12」と言います）  
 彼はミサイルを他の国に送ることができます。  
計算上安全な認証と同様に、無条件の多様性はメッセージの秘密性を提供するかどうかにかかわらず、ブロック暗号のように、またはプレーンテキストメッセージのMACのように機能します。  
複数の仲裁人が必要な場合もあるため、個別に信頼する必要はありません。  
たとえば、機密性のない無条件のコードでは、従来の暗号化システムを使用してメッセージとオーセンティケーターを単純に暗号化することで、計算上安全な機密性を追加できます。  
エラー訂正コードの設計者が特定のエラー回復機能に対して最短のコード長を望んでいるのと同じように、認証コードの設計者は、詐欺確率の特定の限界を達成するために必要なキーの長さを最小限に抑えたいと考えています。  
キーを非武装化せずに人々による武装解除または解体に抵抗する方法で、弾頭にキー制御メカニズムを構築する方法を考え出す必要があります。  
攻撃者がソーシャルエンジニアのメンテナンススタッフをどのように攻撃する可能性があるか、そしてこれを防ぐために何をするかについて考える必要があります。  
バッテリーを交換するために爆弾の武装を解除するメンテナンス担当者がユニバーサルロック解除コードを知らないように、一方向性の要素をどのように導入しますか？  
さらに、危機により一部の武器が許可された場合に備えて、復旧や鍵の更新を行うための実用的なメカニズムが必要です。  
どちらの場合も、無条件のセキュリティと計算によるセキュリティの興味深い組み合わせができあがります。  
  
1970年代後半から、核の指揮統制ビジネスはさらに複雑になり、米国の国家司令当局に対するソビエトの斬首ストライキが兵器庫を無傷で残しておいても役に立たないかもしれないという懸念を抱きました。  
。  
考えは緊張の時にバックアップ制御システムが活性化され、オフィスの所有者またはフィールドの指揮官の組み合わせが共同で武器の武装を許可できるということです。  
この特定のケースは、潜水艦が発射した弾道ミサイルです。  
英国政府は、米国の法理の下で、米国が破壊された場合、潜水艦司令官が兵器を武装できないままになる可能性があり、大統領と彼の合法的な後継者が殺されることを懸念していました。  
役員が同意すれば、ミサイルを発射することができます。  
 ええと、認証キーの半分を2人のユーザーそれぞれに与えるだけかもしれませんが、その場合、元のセキュリティパラメータがいずれかが借用されている場合でも適用する必要があると仮定すると、キーの2倍の長さが必要です。  
これは、現金自動預け払い機のキーを管理する方法です2。  
したがって、より一般的なアプローチは、1979年にBlakleyとShamirによって独立して発明されました[256、1703]。  
。  
これを実装するには、z軸上の点Cを武器に提供する必要のあるロック解除コードとします。  
これで、それらの2つを組み合わせて線の座標を計算し、z軸と交わる点Cを見つけることができます。  
これで、3人の将軍、または2人の将軍と大臣が飛行機と発砲コードCを再構築できます。  
ただし、無条件にセキュリティで保護された認証コードのコンテキストでは、追加は問題ない場合があります。  
秘密分散の紹介は[1829]に、より詳細な説明は[1750]にあります。典型的な軍用アプリケーションでは、2のうちの2つの制御が使用されます。 nは、戦闘の損失があっても、少なくとも2人のキーホルダーが準備ができ、その仕事を行えるように十分に大きくなければなりません。  
たとえば、指揮官の死は彼の代理に鍵の半分を与えるべきではありません、そして誰がいつ誰を撃つか（同じ側で）など、あらゆる種類の骨の折れる問題があります  
銀行はほとんど同じです。高額の支払いを行うには2人の担当者が必要となる場合があり、委任規則では両方のキーが1組の手に渡ることを許可しないように注意する必要があります。  
典型的な例は、海賊が数十の加入者カードを購入し、その秘密のためにリバースエンジニアリングする有料テレビです。  
この裏切り者追跡問題については、著作権の章で詳しく説明します。  
15.5耐タンパー性とPAL  
、ほとんどの米国の核装置を保護するために使用されます。  
PALの開発は1961年頃に始まりましたが、展開に時間がかかりました。  
より複雑なアーミングオプションが導入されたため、コードは4桁から6桁に、最終的には12桁に増加しました。  
。  
。  
どのようなシステムの組み合わせを使用しても、盗まれた武器から泥棒が核収量を取得する能力を否定するペナルティメカニズムがあります。  
この自己破壊手順は、敵の捕獲が脅かされている場合、収量なしで永久に作動不能にします。  
爆弾の輸送物を盗むために「テロリスト」を配備する準備ができている反乱政府が、爆弾の一部（および一部の技術担当者）を犠牲にする準備ができていると想定されています  
許可されたメンテナンスを実行するには、タンパープロテクションを無効にする必要があり、これには別のロック解除コードが必要です。  
保証の目標は[1825]にまとめられています。現在、このような武器を手に入れ、一連の図面を持ち、国立研究所の1つの技術的能力を享受した人でさえ、爆発を成功させることはできないと考えられていますコードを知らなくても。  
必要なケアのレベルの例はいくつかあります。•テストにより、1 mmのチップの破片が空中コマンドポストに搭載された制御装置の保護爆破を生き延びたことが示された後、3Bruce Blairは戦略空軍が新しい教義に抵抗し、大統領および国防長官の継承[255]に嘘をついて、1977年までの '00000000'の権限者認可コード。  
ソフトウェアが書き直され、すべての主要な素材が2つの個別のコンポーネントとして保存され、チップ表面で1 mm以上離れたアドレスに保持されました。 •大統領の背後で持ち運ばれるコマンドデバイスである「フットボール」は、形作られた料金がその保護メカニズムを無効にするために使用される恐れがあるため、それと同じくらい厚いです。  
そのため、アラーム回路にコードメモリをゼロ化するのに十分な時間を与えるために、ある程度の距離が必要になる場合があります。  
武器のテストプロセスには、独立した検証と検証だけでなく、競合する機関による敵対的な「ブラックハット」侵入の試みが含まれます。  
デバイス（弾薬と制御の両方）  
改ざん防止については、銀行カードや電話などのアプリケーションで広く使用されているため、改造については別の章で詳しく説明します。  
さらに微妙なシステムレッスンもあります。  
15.6条約の検証  
たとえば、IAEAと米国原子力規制委員会（NRC）  
興味深い例は、包括的テスト禁止条約[1747]を監視するように設計された耐タンパー性の地震センサーデバイスから来ています。  
 高い確率で検出できます。  
アセンブリ全体が非常に強固であるため、地震計自体がかなり高い確率で改ざんイベントを検出することに依存できます。  
認証プロセスは、広範囲にわたる詐欺を想定しているため、多少複雑になります。  
 ワンタイム認証タグの代わりに使用されました。  
ある当事者は、署名されたメッセージを生成した責任者が不在であったため、署名されたメッセージを常に否認し、署名が偽造された可能性があります。  
また、一方が機器を構築する場合、もう一方は、機能が隠されていると疑います。  
これらの問題の多くは、それ以来、電子商取引で再浮上しています。ハイテク保護メカニズムの開発に巨額の投資が行われているにもかかわらず、原子力制御および安全システムは、他と同じ種類の設計バグ、実装の失敗、不注意な操作に苦しんでいるようです。  
15.7.1原子力事故  
私たちはすでに、国際原子力および放射線事象スケールで74と評価された2つの原子力事故、すなわちチェルノブイリと福島での事故と、それほど深刻ではない事故をいくつか経験しています。  
廃棄物文書が偽造されています。放射線漏れはカバーされています。労働者は、車を制限区域に持ち込むことができるように、入場券を変更しました。妨害行為の報告があった。核警察は、盗難や犯罪による被害の10〜20％しか解決できませんでした[1131]。  
核兵器工場や潜水艦基地を含む防衛核事業の他の場所には、老朽化し​​た施設、無能な請負業者、士気の低さ、プロジェクトの遅延、急騰するコスト、20隻の古い潜水艦の処分を待つ重大な問題が広がっています。まだ燃料を含んでいます[1560]。  
核の保管に関する調査では、核分裂性物質が闇市場に時折現れ、内部告発者が起訴されることで、彼らの安全保障機構がソ連崩壊後にどのように悪化したかを説明した[953]。  
15.7.2サイバー戦争との相互作用  
ここで説明されている改ざん防止メカニズムは、コマンドアンドコントロールチャネル自体が暗号と4を使用した操作に対して無防備になった場合でも、定義されているのは、「計画的かつ拡張された対策の実施を必要とする、広範囲にわたる健康と環境効果のある放射性物質のメジャーリリース」です。サービス拒否攻撃を受ける可能性があります。そして2018年に、トランプ政権はそのような攻撃に応じて核兵器の最初の使用を許可するように教義を変更しました。  
1983年に、国際ソビエトの時代に新しいソビエトの早期警戒システムが機能しなくなり、アメリカがロシアに5つのミニットマンミサイルを発射したと報告しました。  
それはおそらく世界が偶発的な核戦争に至った最も近いものでした（3年前に米国の誤警報もあった）  
AIがあらゆる種類の場所でコマンドチェーンに侵入し、気付かないうちに、はるかに複雑なシステムができた今日、そのようなシステム障害はどのように起こりますか？  
 ミサイル発射を監視し、核爆発を検出し、命令を渡す衛星を含む機能？  
計画、早期警告、または通信システムへのサイバー攻撃も壊滅的な結果をもたらす可能性があるため、武器自体を保護するだけでは不十分です。  
従来の指揮統制ネットワークへの攻撃は、これらのネットワークが核兵器にも使用されている場合、戦略的な脅威と見なされる可能性があります。  
技術的なサイバーセキュリティ対策だけでは十分ではない可能性があります。重要な人物を無能に見せることによって弱体化できるかどうかなど、重大なソフト問題があるためです。  
私は、NATO以外の原子力発電所の信号諜報機関の幹部から個人的に、対立の中で彼らは地域のライバルに「落ち込んだ」と言われました。  
最近では、米国  
そしてそれは宣言された核保有国だけではありません。  
。  
 実際の機能はありません。  
2009年に濃縮ウランの生産量は30％減少し、2010年にはウイルスが発見されました。  
米国政府の関与は、最終的に2012年に認められました[1028]。  
15.7.3技術的な障害  
1つの例は、核兵器削減条約で発見された可能性のある攻撃であり、それが暗号数学の新しい分野の開発–サブリミナルチャネルの研究–につながり、その後著作権マーキングとステガノグラフィーの研究に関連しています。  
カーター政権下で、アメリカはソ連との協定を提案し、両国は大陸間弾道ミサイルの数を検証するために互いに協力することになった。  
したがって、ソビエトは最初のストライキを成功させるために1,000サイロすべてを破壊する必要があり、これは非現実的であると考えられていました。提案された解決策は、サイロがロシアのセンサーパッケージを持ち、ミサイルの有無を検出し、この1ビットの情報に署名し、米国の監視施設を介してモスクワに送信するというものでした。  
（どちらか一方の不正行為を防止したり、他方の不正行為を誤って非難したりするために、他にも多くのセキュリティ要件がありました。詳細については、[1752]を参照してください。）  
システム全体の値は、素数p、素数qがp ffi 1を除算したもの、および次数qのF order pのサブグループのジェネレータgです。  
）  
、およびkはランダムセッションキーです。  
 次に、結果の値rが目的の部分文字列になるまで、kの値を次々に試してみます。  
しかし結局、マスコミで知られるようになった「ミサイルシェルゲーム」は使われなくなりました。  
 統計的手法を使用した。  
冷戦の終結に伴い、検査は衛星ではなく、両側からオブザーバーがいる有人航空機の検査飛行とより密接になっています。  
彼らが悪用される可能性のある方法には、HIVステータスまたは重罪の有罪判決の事実をデジタルパスポートまたはIDカードに入れることが含まれます。  
  
最後に、原子力産業は秘密の素晴らしい歴史を提供しています。  
 ヒロシマとナガサキの装置の設計をソビエト連邦に漏らし、事態はもう一方の極限に向かって揺れた。  
つまり、もしあなたが米国の管轄権の範囲内にあり、核兵器に関連する考えを持っているなら、あなたは保安認可を保持しているか、あるいは核産業で働いていたかどうかに関わらず、それを秘密にしておかなければなりませんでした。  
その後、保護の問題が詳細に検討されたため、事態は大幅に緩和されました。  
「それをどのレベルで分類すればよいですか？  
 ロシア人、彼らは彼らのためにそのデータを持っています。  
ガダ？  
このような問題が解決されるにつれ、多くのテクノロジーが機密解除され、少なくとも概要が公開されました。  
施設の50の建物のうちどれに警報対応部隊が含まれているかなど、妨害行為を促進する可能性のある情報を含め、多くの実装の詳細は秘密にされています。  
偶発的な戦争の可能性を減らすことの利点は、秘密の可能な利益を上回ると考えられていました。  
これはケルクホフの教義の近代的な生まれ変わりであり、19世紀の格言であり、システムのセキュリティはその鍵に依存しなければならず、そのデザインはあいまいなままではありません[1042]。  
9/11以降、多くの政府が生物兵器を使用したテロリストの可能性について話し合い、細菌学、ウイルス学、毒物学、そして実際の医学における研究と教育に規制を課しました。  
「炭疽菌について心配するべきではありません」と英国のトップウイルス学者の一人が私に言った。  
これらのポリシーにより、次回ウイルスがナイル川から降りてきたときにハルツームに公衆衛生の専門家がいない場合は、申し訳ありません。」悲しいことに、2020年の出来事はこの知恵を裏付けています。  
15.9まとめ  
費用に関係なく、武器と核分裂性物質を保護する必要があるという合理的な決定により、他の場所で応用されている多くの数学と科学の発展が促進されました。  
この本の残りの部分には、アラームからアイリスバイオメトリクス、不正開封防止の電子機器からシールまで、他の例が散在しています。  
サイバー攻撃が国の諜報活動、監視、偵察能力を狙うことによって抑止力への信頼を損なう可能性がある場合でも、深刻な不安定化が続く可能性があります。  
そして、アメリカの大統領が1945年以来約12回核の脅威を使ってきたことを考えると（キューバ、ベトナム、イラクは単なるより明白な例にすぎません）  
研究の問題2001年の第1版でこの章の終わりに設定した研究の問題は、「認証コードなど、この領域で開発されたテクノロジーの興味深いアプリケーションを見つけること」でした。第2版では、ブロック暗号のガロアカウンターモードの動作標準化されていましたが、今では普及しています。  
 現在、最も深刻な研究課題は、シリコンとプルトニウムの相互作用でしょう。  
そのような攻撃の脅威はどのようにして核紛争のリスクを増大させるのでしょうか、そしてそれに対して私たちは何ができますか？さらに読む私自身の核兵器の直接の経験はかなり古く、1970年代に原子力対応航空機のアビオニクスに取り組んでいるため、この章は出版された情報源と内部関係者との会話から組み立てられました。  
機密解除の問題についても[2045]で説明されており、PALについて公開されている資料はSteve Bellovinによってまとめられています[217]。  
彼の本[1749]は、この章で説明するほとんどの技術資料の参照として最適です。  
原子力施設における制御障害は、多くの場所で文書化されています。  
問題の最良かつ最新の調査は、公会計委員会の2018年報告書「国防省の核計画」[1560]に記載されています。