SSL の安全性評価報告書

2001 年 12 月 28 日

株式会社 日立製作所

1. はじめに

SSL (Secure Socket Layer) は, トランスポートレイヤの代表的な暗号通信プロトコルで, 特に Web をベースとする e コマース等で用いられている. SSL では通信におけるセキュリティを確保するため, DES や RC4 等の共有鍵暗号を用いたデータ暗号化機能と，RSA や DSS 等の公開鍵暗号を用いたサーバ認証およびクライアント認証機能を，また，SHA や MD5 等のハッシュ関数を用いてデータ改ざん検知機能を提供している．本報告は，暗号通信プロトコルの安全性を判定するための基礎資料として，この SSL に関する脆弱性を調査した結果を述べるものである.

2. 調査方法

2.1. 調査対象

SSL は，現在の Web サーバで用いられているバージョンである“ SSL バージョン 3.0 ”と，現在 IETF (Internet Engineering Task Force) で RFC として仕様がまとめられている“ TLS バージョン 1.0 ”が存在する．本報告においては，この 2 つのバージョンを対象として調査を実施した．本報告では，以下に示すコンピュータセキュリティ関連の情報源をもとに，これらのプロトコルを利用したアプリケーションに対して現在までに報告された既知の脆弱性の調査を実施した.

・CERT/CC Advisories
http://www.cert.org/advisories/
1988/12 から 2001/10 までに CERT/CC から公開された 255 件の脆弱性情報

・Microsoft Security Bulletin
http://www.microsoft.com/technet/security/current.asp
http://www.microsoft.com/japan/technet/security/current.asp
1998/6 から 2001/10 までに Microsoft 社から公開された 231 件の脆弱性情報

・CIAC
http://ciac.llnl.gov/cgi-bin/index/bulletins
1989/4 から 2001/10 までに，Computer Incident Advisory Capability から公開された 734 件の脆弱性情報

・CVE
http://cve.mitre.org/
従来 CERT アドバイザリやその他ベンダが提供する脆弱性情報は, 同一の脆弱性であっても各情報源ごとに脆弱性の呼称が異なっていることが多く，脆弱性情報やセキュリティ情報同士の同一性を確認することが難しかった.“ CVE(Common Vulnerabilities and Exposures) ”はこのような脆弱性情報ならびにセキュリティ情報の関連付けを行うことを目的とするディレクトリである．本報告書では，参考として CVE 識別子を付記した.

2.2. 調査方法

本報告では，上記の情報源が提供するサーチ機能を使用して，SSL に関連する脆弱性情報を抽出した．また，抽出した脆弱性情報に関しては，以下の観点より分類・整理を行なった．

・脅威の概要
・影響および原因
・脅威のレベル(高：システムへの侵入，中：機密データ漏洩，低：サービスレベルの低下)
・対策
・その他のコメント

3. 調査結果

3.1. 概要

1988/12～2001/10 まで，SSL に関係する脆弱性情報として報告されたものは，全部で 16 件存在する．これらは以下の 6 種類の問題に大別される．

(1) SSL 実現ライブラリのバッファオーバフロー問題

SSL の機能を実現するライブラリのプログラムバグにより発生する問題である．本問題により，ライブラリを利用したサーバプログラムを用いてサーバ計算機の無権限利用が行なわれる危険性がある．本問題に属する脆弱性の報告は，以下の 3 件である．

CIAC L-141 (September 12, 2001)
CA-1999-15 (December 13, 1999)，CIAC K-011 (December 21, 1999)
CA-1998.07 (June 26, 1998)，CIAC I-066 (June 26, 1998)

(2) SSL アプリケーションの実装ミス(証明書処理)

SSL アプリケーションのプログラミングにおいて，証明書の検証方法により発生する問題である．本問題により，サーバあるいはクライアントの成りすましが発生する危険性がある．本問題に属する脆弱性の報告は，以下の 4 件である．

MS01-027 (May 16, 2001), CIAC L-087 (May 23, 2001)
MS00-039 (June 05, 2000), CA-2000-10 (June 6, 2000), CIAC K-04 (June 6, 2000)
CA-2000-08 (May 26, 2000), CIAC K-047 (June 13, 2000)
CA-2000-05（May 12, 2000）, CIAC K-040 (May 15, 2000)

(3) SSL アプリケーションの実装ミス(Web セッション管理)

SSL アプリケーションのプログラミングにおいて，クッキー等の Web のセッション管理に使用する機構の使い方により発生する問題である．本問題により，秘密にすべき情報が，サーバあるいはクライアントに成りすました第三者に漏洩する危険性がある．本問題に属する脆弱性の報告は，以下の 3 件である．

MS00-080 (October 23, 2000), CIAC L-010 (October 24, 2000)
MS00-076 (October 12, 2000)
CIAC I-082 (August 6, 1998)

(4) SSL アプリケーションの実装ミス(その他)

SSL アプリケーションのプログラミングにおいて，(2), (3)に示した以外の原因により発生した問題である．本問題に属する脆弱性の報告は，以下の 2 件である．

MS01-036 (June 25, 2001)，CIAC L-101 (June 26, 2001)
CIAC L-068 (April 6, 2001)
MS99-053 (December 02, 1999)
CIAC J-062 (September 1, 1999)

(5) 運用関連

SSL で使用する X.509 証明書の運用管理により発生した問題である．本問題に属する脆弱性の報告は，以下の１件である．

CA-2001-04 (March 22, 2001)

(6) Web コンテンツ関連

Web コンテンツの内容により発生する問題である．本問題に属する脆弱性の報告は，以下の 1 件である．

CA-2000-02 (February 2, 2000), CIAC K-021 (February 3, 2000)

3.2. 詳細報告

本章では，調査した脆弱性の詳細を説明する．

3.2.1. SSL 実現ライブラリに関する問題

3.2.1.1. RSA BSAFE SSL-J 3.X の脆弱性

【概要】

RSA BSAFE SSL-J 3.x の SDK に，リモートユーザの認証なしに SSL セションを確立することを許す脆弱性が存在する．

【影響】

このライブラリを使って暗号化された SSL セションを生成するソフトウェアは, 認証されていないユーザのシステムアクセスを許してしまう．

【原因】

ライブラリの設計ミス

【脅威のレベル】

高

【対策方法】

ライブラリをバージョンアップする

【出典】

CIAC L-141 (September 12, 2001)

3.2.1.2. CERT/CC SSH デーモン，RSAREF2 ライブラリ，バッファオーバフロー問題

【概要】

RSAREF2 中の脆弱性により，ネットワーク経由で任意のコードを実行することが可能となる

【影響】

サービスの権限での不正アクセスが可能になる

【原因】

RSAREF2 ライブラリの実装に問題がある．

【脅威のレベル】

高

【対策方法】
ライブラリをバージョンアップする

【出典】
CA-1999-15 (December 13, 1999), CIAC K-011 (December 21, 1999)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0834

3.2.1.3. PKCS#1 の利用に関する弱点について(SSL 実装上の弱点)

【概要】
RSA ラボラトリの Public-Key Cryptography Standard #1 (PKCS#1)製品を利用して，インタラクティブにセション確立を行い，かつサーバが返送するエラーメッセージに失敗に該当する状態があるプロトコルを実装したサーバでは， SSL セッションの中身を解読される危険性がある.

【影響】
SSL セッションの中身を解読される危険性がある.

【原因】
RSA ラボラトリの Public-Key Cryptography Standard #1 (PKCS#1)を実装しているいくつかの製品の弱点(バッファオーバフローと思われるが詳細は不明).

【脅威のレベル】
中

【対策方法】
ライブラリをバージョンアップする

【出典】
CA-1998.07 (June 26, 1998), CIAC I-066 (June 26, 1998)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0007

3.2.2. SSL アプリケーションの実装に関する問題(証明書処理関連)

3.2.2.1. Microsoft Web サーバー証明書検証の問題により Web サイトの偽装が可能になる

【概要】

デジタル証明書を検証方法と，Internet Explorer のアドレスバー表示の偽装により，Web サイトの偽装が可能になる

【影響】

信頼された Web サイトに成りすますことができてしまう.

【原因】

Web サーバのデジタル証明書を検証する方法に関する脆弱性証明書の CRL(certificate revocation list)チェックが有効になっている場合，以下のチェックのいくつか，または全ての確認が行われない.

・証明書の有効期限の確認
・証明書に記載されているサーバ名と実際のサーバ名との照合
・証明書の発行者の信頼性に関する確認

成りすましたサイトとの SSL セッション内で IE アドレスバーに異なる Web サイトの URL 表示に関する脆弱性 Web ページが，Internet Explorer のアドレスバーに別の Web サイトの URL を表示してしまう.

【脅威のレベル】

中

【対策方法】

Internet Explorer をバージョンアップする．また，不審なサイトにはアクセスしない.

【出典】

MS01-027 (May 16, 2001), CIAC L-087 (May 23, 2001)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0338
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0339

3.2.2.2. Microsoft Internet Explorer SSL 証明書確認操作の問題

【概要】

Microsoft Internet Explorer の X.509 証明書取り扱いの不備をつき，不審な証明書に対する警告を無効にする.

【影響】

偽の証明書を使用しているサーバを本物のサーバと誤認識させることができる.

【原因】

Internet Explorer が SSL 証明書のサーバ名，有効期限の確認において，画像あるいは，フレームのいずれかがセキュア Web サーバに接続している場合，IE は，サーバの SSL 証明書が信頼できる root 認証局によって発行されていることのみを確認し，サーバ名や有効期限の確認は行わないことと，最初の確認において SSL 証明書が正しいと判断した場合，同じ IE セション中で，新たな SSL セションを同じサーバとの間に確立するならば，SSL 証明書を再度確認しない.

【脅威のレベル】

中

【対策方法】

Internet Explorer をバージョンアップする．また，不審なサイトにはアクセスしない.

【出典】

MS00-039 (June 05, 2000), CA-2000-10 (June 6, 2000), CIAC K-04(June 6, 2000)

3.2.2.3. Netscape Navigator 警告メッセージ問題

【概要】

Netscape Navigator の X.509 証明書取り扱いの不備をつき，不審な証明書に対する警告を無効にする.

【影響】

偽の証明書を使用しているサーバを本物のサーバと誤認識させることができる.

【原因】

Netscape のセションにおいて,「ホスト名は証明書の名称と一致しない“ hostname does not match name in certificate ”」というエラーに対して，ユーザが「次へ“ continue ”」をクリックしてしまうと，証明書を利用するサーバが，正当なサーバではなく，他のサーバ(他ホスト名や他 IP アドレス)であるにも関わらず，その後，Netscape のセションにおいては，証明書を誤って有効であると取扱ってしまうことにある.

【脅威のレベル】

中

【対策方法】

Netscape Navigator をバージョンアップする．また，不審なサイトにはアクセスしない.

【出典】

CA-2000-08 (May 26, 2000), CIAC K-047 (June 13, 2000)

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0517

3.2.2.4. Netscape Navigator における SSL セション取扱い問題

【概要】

Netscape Navigator の SSL セション取扱い方法の不備をつき, 基本的な SSL 機能のうちの１つ(意図した Web サーバと実際に通信しており，偽物ではないことを保証する機能)を効果的に無効化する.

【影響】

「無効な SSL 証明書」警告表示することなく，不正な SSL セションを利用することができてしまう．このため SSL プロトコルにより通信を保護していたとしても，攻撃者はユーザに，本物の Web サーバではなく，攻撃者の Web サーバに秘密情報(クレジットカードデータやパスワードなど)を送付させることができる.

【原因】

Netscape Navigator は，Web サーバとの間で SSL セションを確立する時に，証明書の条件(*)を正しく確認する．しかし，この SSL セションがまだ有効となっている場合，そのサーバの IP アドレスに対して接続する全ての HTTPS は，有効となっているセションの継続であると仮定してしまうという欠陥がある(証明書の条件を再度確認していない)．すなわち，Navigator は，現在利用しているセションに対して，ホスト名を比較する代りに，IP アドレスを比較する．同じ IP アドレスに対して複数のホスト名がある場合，セキュリティ上の脅威となる.

【脅威のレベル】

中

【対策方法】

Netscape Navigator をバージョンアップする．また，不審なサイトにはアクセスしない.

【出典】

CA-2000-05 (May 12, 2000), CIAC K-040 (May 15, 2000)

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0406

3.2.3. SSL アプリケーションの実装に関する問題(Web セッション管理)

3.2.3.1. Microsoft IIS 4.0/5.0 Session ID Cookie 生成における脆弱性

【概要】

SSL で保護されたサイトに対する Session ID cookie を，悪意のあるユーザに不正に取得されてしまう.

【影響】

SSL で保護されたサイトに対して悪意のあるユーザがなりすましてセッションを実行する危険性がある.

【原因】

Internet Explorer は，同じ Web サイト上の SSL で保護されたセキュアなページと，セキュアではないページで同じ Session ID cookie を使用するため.

【脅威のレベル】

中

【対策方法】

Internet Explorer および，IIS サーバをバージョンアップする．また，不審なサイトにはアクセスしない.

【出典】

MS00-080 (October 23, 2000), CIAC L-010 (October 24, 2000)

3.2.3.2. Microsoft IE 4.x, 5.x における Cached Web Credentials 問題

【概要】

SSL で保護されたサイトに対するユーザ ID とパスワードを，悪意のあるユーザに不正に取得されてしまう.

【影響】

SSL で保護されたサイトに対して悪意のあるユーザがなりすましログインを実行する危険性がある.

【原因】

セキュアな Web ページに対する認証として基本認証(ユーザ ID とパスワード)を利用している場合, 同一サイトへの認証操作を低減するために, IE は, そのユーザの ID とパスワードをキャッシュし, これを利用している．設計上，IE は，サイト上のセキュアな Web ページに対してのみキャッシュ

した認証情報を送信すべきである．ところが，実装上，同一サイトのセキュアではないページに対しても，同様に基本認証情報を送信してしまう．

【脅威のレベル】
中

【対策方法】
Internet Explorer をバージョンアップする．また，不審なサイトにはアクセスしない．

【出典】
MS00-076 (October 12, 2000)

3.2.3.3. HP-UX Netscape Server の SSL に関するセキュリティ上の弱点

【概要】
HP9000 シリーズ 7/800 上で稼動する HP-UX10.X と 11.00 で，攻撃対象となるサーバに 100 万回近くのメッセージを繰り返し送り，その応答を調べることで，暗号化されたセションで使用されている暗号鍵を類推することが可能となる．

【影響】
SSL セッションの中身を解読される危険性がある．

【原因】
SSL をサポートする Netscape サーバ製品の RSA データセキュリティ暗号アルゴリズムに関わる部分でセキュリティ上の弱点がある．

【脅威のレベル】
中

【対策方法】
HP-UX 版 Netscape Server をバージョンアップする．また，不審なサイトにはアクセスしない．

【出典】
CIAC I-082 (August 6, 1998)

3.2.4. SSL アプリケーションの実装に関する問題(その他)

3.2.4.1. Microsoft LDAP SSL で公開される機能がパスワードの変更を可能にする

【概要】

「ディレクトリプリンシパルがドメインユーザで」かつ,「データ属性がドメインパスワードで」ある場合，その変更要求者の権限確認に失敗してしまうために，他ユーザによりユーザのドメインログインパスワードを変更されてしまう可能性がある.

【影響】

他ユーザのログオンを妨害することにより，サービスを利用できない状態に陥れる，もしくはユーザのアカウントでログインし，そのユーザの持つ権限を取得する.

【原因】

LDAP SSL セッションをサポートするよう設定された LDAP サーバでのみ利用可能な LDAP 機能,ディレクトリプリンシパルのデータ属性の変更に関連するもので，仕様上，その変更要求を完了する前にユーザ権限確認を行うことになっているが,「ディレクトリプリンシパルがドメインユーザで」かつ,「データ属性がドメインパスワードで」ある場合，その変更要求者の権限確認に失敗してしまうため.

【脅威のレベル】

高

【対策方法】

Microsoft LDAP サーバをバージョンアップする.

【出典】

MS01-036 (June 25, 2001)，CIAC L-101 (June 26, 2001)

3.2.4.2. Cisco VPN3000 Concentrator における TELNET の脆弱性

【概要】

Cisco VPN 3000 series concentrators 上で動作する SSL と telnet サービスの脆弱性により，DoS 攻撃をかけられるとシステムがリブートする.

【影響】

システムがリブートし，通信ができなくなる.

【原因】

サービスの実装方式に問題があった.

【脅威のレベル】
低

【対策方法】
Cisco VPN 3000 series concentrators のファームウェアをバージョンアップする.

【出典】
CIAC L-068 (April 6, 2001)

3.2.4.3. Microsoft IIS/Site Server マルチスレッド SSL ISAPI フィルタ問題

【概要】
マルチスレッド化されたアプリケーションがある特定条件下で SSL ISAPI の呼び出しを行った場合に，処理中のデータの一部がプレーンテキスト(暗号化されていないデータ)としてデータ所有者に送り返されてしまう.

【影響】
通信路が盗聴されていた場合，機密情報が漏洩する可能性がある.

【原因】
SSL ISAPI フィルタは，同時使用をサポートする IIS の機能として提供されている．この同時使用の状態で同期問題が発生すると，競合状態を引き起こし，プレーンテキストの格納されたバッファのデータが漏えいしてしまう.

【脅威のレベル】
中

【対策方法】
Cisco VPN 3000 series concentrators のファームウェアをバージョンアップする.

【出典】
MS99-053 (December 02, 1999)

3.2.4.4. Netscape Enterprise and FastTrack Web Servers のバッファオーバフロー

【概要】
Netscape Enterprise and FastTrack Web Servers でバッファオーバフローが発生する.

【影響】
サービスの権限での不正アクセスが可能になる

【原因】
サービスの入出力ルーチンの実装方法に問題がある.

【脅威のレベル】
高

【対策方法】
Netscape Enterprise and FastTrack Web Servers をバージョンアップする.

【出典】
CIAC J-062 (September 1, 1999)

3.2.5. 証明書運用に関する問題

3.2.5.1. “ Microsoft Corporation ”の名を騙った証明書

【概要】

VeriSign 社から, 2001 年 1 月 29 日および 30 日, VeriSign Class 3 (VeriSign Commercial Software Publishers CA)により署名された"Microsoft Corporation" の名前の記載された偽のデジタル証明書が 2 枚発行された.

【影響】

ユーザが，これらの偽証明書により署名されたプログラムの実行を試みた場合，警告ダイアログが表示されるが，警告ダイアログの表示だけでは，正規の証明書によるものであるかどうかを判定できない.

【原因】

認証機関(Certificate Authority)が，証明書受領者の確認に失敗したことに起因している．Verisign 社は，既に問題となる証明書を失効するための手続きを行っている．ところが，Internet Explorer では，これらの証明書の失効を自動的に検証しないため，修正プログラムがインストールされるまでの間は，これらの証明書の悪用を防ぐには不十分な状況にある.

【脅威のレベル】

中

【対策方法】

ブラウザをバージョンアップする.

【出典】

CA-2001-04 (March 22, 2001)

3.2.6. Web コンテンツに関する問題

3.2.6.1. Web システムにおける不正な HTML タグ問題

【概要】

SSL セッションにおいて，正規の HTML タグ(HTML を記述するための符号)の中に，悪意を持った HTML タグ(例えば，Java スクリプトなど)を紛れ込ませる．

【影響】

ブラウザを介して，クライアント上の情報が盗まれたり，クライアントのアクセスすることのできる Web サーバ上の情報が盗まれるといった被害が発生する．

【原因】

非 SSL URL への接続を試みる不正なコードは，「安全ではないコネクションである」と行ったメッセージ警告を挙げるかもしれない．SSL は不正なコードならびに，このコネクション上を流れるデータを暗号化する．SSL により覗き見されることなく，クライアントとサーバの通信を行うことができるが，転送されるデータの正当性を確認することはできない．また，クライアントとサーバ間の通信が正規の通信であるため，SSL 自身がなんらかの警告を挙げることはない．このため攻撃者は，SSL 機能を持った Web サーバを稼動させておくことにより(SSL 機能を持ったサイトに接続する)，この警告を回避することができてしまう．

【脅威のレベル】

中

【対策方法】

ブラウザをバージョンアップする．

【出典】

CA-2000-02 (February 2, 2000), CIAC K-021 (February 3, 2000)

4. 考察

(1) SSL3.0 と TLS1.0 のセキュリティ強度の差異について

TLS バージョン 1.0 は，従来 Netscape Communications 社が提唱してきた SSL バージョン 3.0 をベースに，IETF(Internet Engineering Task Force)において標準化が行われている規格である．厳密には両者の間に互換性がないが，仕様の違いは細かなパケットフォーマットの変更や，利用可能な暗号方式等の追加のみである．

3 章において報告した調査結果からは, SSL および TLS のプロトコル仕様に起因する脆弱性は確認されていない．このため，SSL から TLS に移行することにより解消されるセキュリティ問題は特に存在しないと考えられる．

(2) プロトコルの使い分けについて

上記で述べたように，SSL3.0 と TLS3.0 は，厳密には互換性がないものの，プロトコル仕様的にはほとんど差異がない．しかし，TLS1.0 では，AES をはじめとする新しい暗号方式への対応を予定しているため，今後のシステム構築には TLS1.0 を利用することが望ましい．

(3) TLS1.0 の改訂について

現在 IETF では，TLS1.0 の改訂版を検討中である．本改訂版は，2002/2 にドラフトが出来る予定であるが, 新しい暗号方式のサポート等が中心であり, 大幅な変更は予定されていない模様である．

以上