Vol.2012-DPS-150 No.36
Vol.2012-CSEC-56 No.36
2012/3/1

不正な証明書を用いた通信への対策について

榊原裕之[†]　　桜井鐘治[†]

企業等の組織において，インターネットを経由した情報漏洩への対策が課題になっている．様々な情報漏洩の手段があるが，その一部としてフィッシングやマルウエアが挙げられる．ユーザ側のフィッシング対策として，Web サイトとブラウザ間の正常な SSL(Secure Sockets Layer)接続の確認が推奨されているが，近年，マルウエアにより攻撃者が生成した CA(Certification Authority)証明書が計算機に埋め込まれ，この CA 証明書で正しく検証可能な自製のサーバ証明書を用いたフィッシングサイトへ正常に SSL 接続する事象が報告された．また，情報漏洩で問題になっている Advanced Persistent Threats におけるマルウエアと Command & Control サーバ間の通信で SSL を用いることがある．従って，情報漏洩の被害を低減するために組織における不正な SSL 通信への対策が必要である．本稿では，組織における外部との不正な SSL 通信への対策を検討し，組織の管理者が許可しない証明書のネットワークへの流入を監視する対策について考察した．

Countermeasures for unwanted communication with certificates

Hiroyuki Sakakibara[†] and Shoji Sakurai[†]

In an organization such as an enterprise, taking countermeasures against information leaks via the Internet is a challenge. Various ways of information leaks include Phishing and malware. Checking legitimate SSL(Secure Sockets Layer) communication between a browser and a Web site by an end user is recommended as a countermeasure for Phishing. However, recently it was reported that a CA(Certification Authority) certificate issued by an attacker was implanted in a trust store of a user computer by a malware and a Phishing mail guided the user to a Phishing Web site which supports SSL. On this site the user was not able to notice that the site was rogue, because the server certificate was validated with the CA certificate in question and the result of validation was legitimate. Likewise it was reported that in Advanced Persistent Threats which cause information leaks some of malwares communicate with a Command & Control server over SSL. Therefore countermeasures against unwanted SSL communication between an organization and the Internet are needed for reducing damage from information leaks. In this paper, we propose detection of a certificate which an organization does not accept by monitoring communication and warning to a user communicating with the certificate in question.

1. はじめに

企業等の組織において，インターネットを経由した情報漏洩への対策が課題になっている．情報漏洩の方法は様々であるが，その手段の一つとして，フィッシングが挙げられる．例えば，組織から，物品の購入や鉄道の切符を予約するなどインターネット上の Web サイトを活用する機会があり，模倣サイトによるフィッシングの攻撃対象となる．

エンドユーザ（以下ユーザ）向けフィッシング対策として，Web サイトで情報を入力する場合は，Web サイトが SSL(Secure Sockets Layer) [1]に対応しており，ブラウザに鍵アイコンが表示されていることを確認する，などの対応が推奨されている[2]．この対策は，次の考え方に基づいている．SSL は公開鍵証明書（以下，証明書）に基づいた通信相手の認証を採用している．一般的に，認証局(CA :Certification Authority)は Web サイトの運営者の正当性を審査し SSL サーバ証明書（以下サーバ証明書）を発行する．SSL 対応の Web サイト(https://)にブラウザで接続し，ブラウザにより Web サイトのサーバ証明書の正当性が検証された場合にブラウザに鍵アイコンが表示されるため，鍵アイコンの表示を確認することで正当な Web サイトに接続していると判断する．CA による審査に基づきサーバ証明書が発行されるため，フィッシングを行う攻撃者（犯罪者）の Web サイトは審査に通らないであろうという前提のもとに成り立つ対策である．

サーバ証明書の正当性に基づくフィッシング対策を逆手にとり，審査が緩い一部の CA により発行された正規のサーバ証明書を持つフィッシングサイトが運営されるケースが現れ，対策として厳密な審査により発行される EV(Extended Validation)証明書が考案された[3]．EV 証明書に対応した Web サイトに接続した場合は，ブラウザはアドレスバーを緑色に表示するため，Web サイトの安全性を確認できる仕組みである．しかしながら，全ての Web サイトが EV 証明書を採用しているわけではなく，通常のサーバ証明書を採用している Web サイトは一般的である．

攻撃者は，CA による審査を回避するため，CA からサーバ証明書の発行を受けるのではなく，自製することがある．しかし，自製のサーバ証明書は，ユーザの計算機のトラストストア（ブラウザ等が信頼する証明書を保存する領域）に保存されている CA 証明書による検証が失敗するため，ユーザに不正な Web サイトと判断される．ところが，近年，マルウエアにより不正な CA 証明書が計算機に埋め込まれ，不正なサーバ証明書を適用したフィッシングサイトへ正常に SSL で接続する事例が報告された[4]．

また，情報漏洩が問題となっている APT(Advanced Persistent Threats)においても一部

[†] 三菱電機株式会社　情報技術総合研究所
Information Technology R&D Center, Mitsubishi Electric Corporation

Vol.2012-DPS-150 No.36
Vol.2012-CSEC-56 No.36
2012/3/1

のマルウエアは通信に SSL を用いており[5], 自製による不正なサーバ証明書が用いられていると推測される.

本稿では，情報漏洩の原因となるフィッシングやマルウエアが用いる不正な SSL 通信への対策として，組織の管理者が許可しない証明書の流入を監視することによる対策について提案する. 2 章では, 不正なサーバ証明書を悪用したフィッシングの通信，及び，マルウエアの通信について述べ，これらに対し 3 章では従来の対策を，4 章では提案する対策を述べる．5 章で考察を述べ，6 章でまとめる.

2. 不正なサーバ証明書を悪用した通信

不正なサーバ証明書を悪用したフィッシングの通信，及び，マルウエアの通信について述べる.

2.1 フィッシング

EV 証明書の登場により，CA からサーバ証明書の発行を受けたフィッシングサイトは減ったとされるが[2]，マルウエアにより自製の CA 証明書を標的の計算機に埋め込み，自製のサーバ証明書を適用したフィッシングサイトへ，ブラウザが証明書の警告を表示すること無しに接続させる事例が報告されている[4]．今後，この様な自製のサーバ証明書を適用したフィッシングサイトがさらに出現する可能性がある．また，CA が攻撃を受け不正なサーバ証明書が発行された事例が報告されている[2][6].
本節では，不正なサーバ証明書によるフィッシングについて述べる.

2.1.1 自製サーバ証明書を使用しブラウザが警告を表示するケース

攻撃者はサーバ証明書を CA から取得するのではなく，自製しフィッシングサイトに設定する. ユーザがフィッシングメールに記載された URL をクリックしブラウザでフィッシングサイトにアクセスした場合，CA からサーバ証明書の発行を受けていないため，証明書に問題があるという警告が表示される．[7]の事例が該当する.

フィッシングメールに「警告が表示された場合でも，暗号化は実施されるので問題無い」, 等とユーザを騙して接続させる指示が書かれていた場合, ユーザのセキュリティ意識が低い場合はそのまま接続する可能性がある.

2.1.2 自製サーバ証明書を使用しブラウザが警告を表示しないケース

攻撃者はサーバ証明書を自製しフィッシングサイトに設定する．さらに攻撃者は，自製したサーバ証明書の CA 証明書を，攻撃対象のユーザのトラストストアにインストールさせる．この CA 証明書も自製であるが，攻撃対象のユーザのトラストストアにインストールさせる方法として以下の 2 つが考えられる.

・詐称による自製 CA 証明書のインストール方法

攻撃者は，例えば図 1 の手順で，自製 CA 証明書をユーザのトラストストアにインストールさせフィッシングを行う.

① 攻撃者は，自製 CA 証明書と自製サーバ証明書を生成する.
② 攻撃者は，生成した自製 CA 証明書と自製サーバ証明書をフィッシングサイトに設定する.
③ 攻撃者は, 自製 CA 証明書を添付したフィッシングメール A をユーザに送信する.
④ ユーザは，フィッシングメール A の文面に騙されて，自製 CA 証明書を計算機のトラストストアにインストールし保存する.「○○システムを利用するためには添付の証明書をインストールする必要がある」などユーザを騙すメールの文面が考えられる.
⑤ 攻撃者は，③とは別の送信者（サービス提供者）を装い，フィッシングサイトに接続を促すフィッシングメール B を送付する．メールの本文にはフィッシングサイトの URL が記載されている.
⑥ ユーザは，⑤のフィッシングメール B の URL を参照しフィッシングサイトにブラウザでアクセスする．この時，自製 CA 証明書がユーザの計算機のトラストストアにインストールされているため，自製サーバ証明書の検証が成功し，ブラウザが警告を表示すること無しに SSL 通信が行われる.

③と⑤のフィッシングメールは別々の送信者を装ってよく，③の自製 CA 証明書をインストールさせるために騙しやすい送信者を装えばよい．③と⑤のメールの内容も関連付けは必要無い．例えば，③は情報システム部門からのメールで，⑤は事務用品

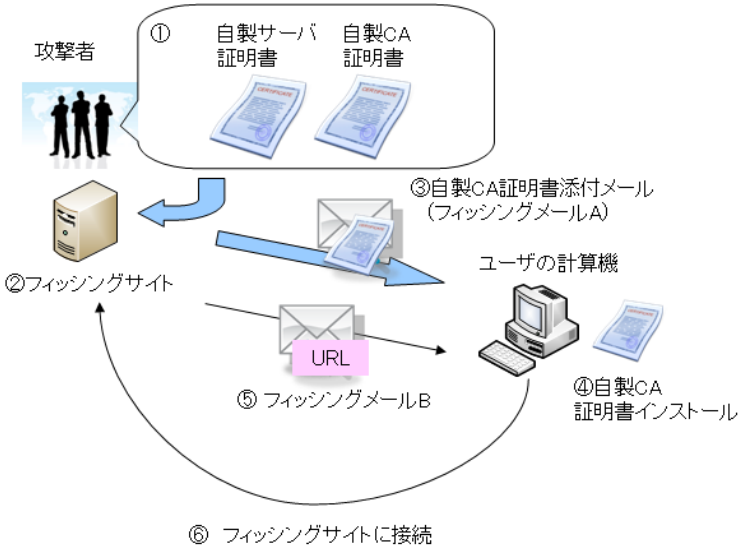

図 1 詐称による自製 CA 証明書のインストール

Vol.2012-DPS-150 No.36
Vol.2012-CSEC-56 No.36
2012/3/1

購入 Web サイトからのメールを装う．一度③で自製 CA 証明書をインストールさせてしまえば，攻撃者は様々なサービス提供者を装った⑤のフィッシングメール B を送付し，ユーザに各々のフィッシングサイトにおいてブラウザによる警告無しに正常な SSL 通信を行わせることが可能となる．

・マルウエアによる自製 CA 証明書のインストール方法

マルウエアにより自製の CA 証明書がトラストストアにインストールされる．例えば[4]の事例においては，マルウエアにより，攻撃者の自製 CA 証明書がトラストストアにインストールされるため，フィッシングサイトにおける攻撃者の自製サーバ証明書が正しく検証される．例えば，図 2 のような手順でフィッシングを行う．

①，②のステップは図 1 に同じである．

③　攻撃者は，自製 CA 証明書をインストールするマルウエア付きフィッシングメール A をユーザに送信する．

④　ユーザは，フィッシングメール A の文面に騙されて，添付ファイルを開くとマルウエアにより自製 CA 証明書が計算機のトラストストアにインストールされる．この時，マルウエアは計算機上のソフトウエアや OS の脆弱性を悪用する．

⑤，⑥のステップは図 1 に同じである．

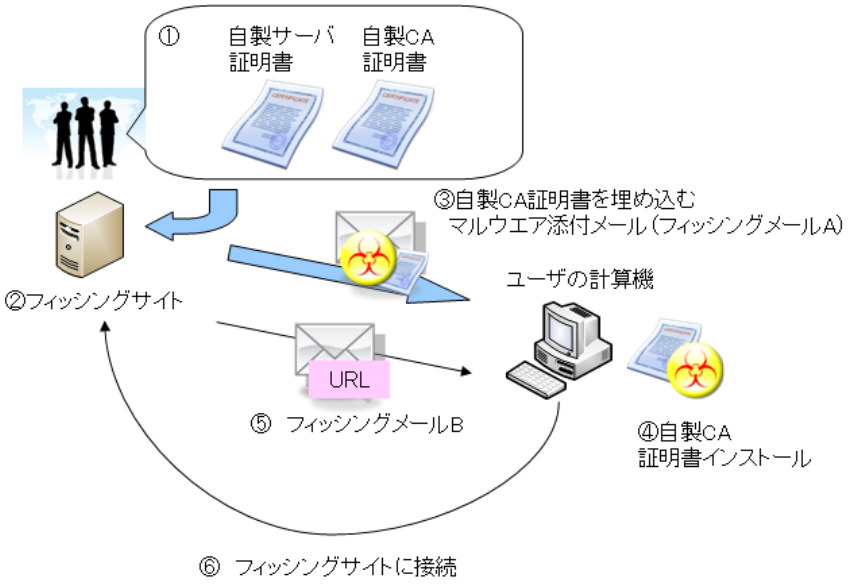

図 2　マルウエアによる自製 CA 証明書のインストール

詐称による自製 CA 証明書のインストール方法，マルウエアによる自製 CA 証明書のインストール方法共に，手順③，④においてフィッシングメールの文面に騙されて指示に従った結果，自製 CA 証明書が計算機のトラストストアにインストールされる．近年の APT における標的型メールは，最初に，標的とする組織と交流があるセキュリティ対策が弱い別の組織を侵攻し，メール情報を窃取し，このメールの発信元に成りすましてメールを送ることがあるとされる[5]．従って，これらの方法における③において攻撃者が同じ手口を使用した場合は，ユーザは信頼する組織からのメールなのでメールの文面を信用し指示に従い，その結果，自製 CA 証明書のインストールに成功する可能性がある．

2.1.3 CA を攻撃し入手した正規のサーバ証明書を使用しブラウザが警告を表示しないケース

攻撃者は CA を攻撃し，CA から正規のサーバ証明書を不正発行させた事例がある[2][6]．攻撃者は不正発行されたサーバ証明書をフィッシングサイトに設定後，ユーザにフィッシングメールを送付しフィッシングサイトに誘導する．この場合には，計算機のトラストストアに保存されている正規の CA 証明書がサーバ証明書の検証に使用されるため，フィッシングサイトへの SSL 接続においてブラウザは警告を表示しない．

2.2　マルウエア

組織内とインターネット間において，証明書を用いた不正な通信は，組織内とフィッシングサイトとの SSL 通信だけではない．近年では，APT においてマルウエアが行う通信の約 3 割が SSL(HTTPS)であったという報告がされている[5]．

2.2.1 自製サーバ証明書を使用するケース

マルウエアと C&C(Command & Control)サーバ間の SSL 通信は，マルウエアが C&C サーバのサーバ証明書を受け入れれば成立する．C&C サーバとマルウエアは同じ攻撃者により運用されるので，サーバ証明書は攻撃者による自製で良い．従って，APT が使用するサーバ証明書は，自製証明書であることが多いと予想する．

2.2.2 CA を攻撃し入手した正規のサーバ証明書を使用するケース

攻撃者は CA を攻撃し，CA から正規のサーバ証明書を不正発行させ，これを C&C サーバのサーバ証明書として使用する．

3.　不正なサーバ証明書を悪用した通信への従来の対策

3.1　フィッシングへの対策

3.1.1 自製サーバ証明書を使用したフィッシングへの対策

本節では，2.1.1，2.1.2 で述べた自製サーバ証明書を使用したフィッシングへの従来の対策を述べる．

Vol.2012-DPS-150 No.36
Vol.2012-CSEC-56 No.36
2012/3/1

3.1.1.1. **ユーザの教育**

Web サイトに接続しようとした際に，ブラウザが証明書についての警告を表示した場合は接続しないようにユーザを教育する．さらに，警告無しで接続でき，鍵アイコンが表示されたとしても，URL が不正ではないか，Web サイトのコンテンツが怪しくないかを判断する．そのために，組織のシステム管理者は判断に必要なマニュアルを作成し，ユーザに対して教育を行う．

3.1.1.2. URL **フィルタリング**

ユーザがブラウザでアクセスする URL におけるホスト名を，ホワイトリストやブラックリストによるフィルタリングで制限する．

3.1.1.3. EV **サーバ証明書が使用されていることの確認**

EV サーバ証明書は，サーバ証明書発行時に認証局による厳格な審査を通過したものだけに発行される証明書である．ブラウザで EV サーバ証明書を使用した Web サイトにアクセスすると，アドレスバーの色が変わり，安全であることが示される．ユーザは，SSL 対応の Web サイトに接続した際に，ブラウザが警告の表示無しでコンテンツを表示したこと，鍵アイコンの表示とアドレスバーの色を確認することで，フィッシングサイトではない安全なサイトに接続していると判断する．

3.1.2 CA **を攻撃し入手した正規のサーバ証明書を使用したフィッシングへの対策**

3.1.2.1. **ユーザの教育**

3.1.1.1 と同様に，ブラウザの警告無しで Web サイトに接続でき，その際に鍵アイコンが表示されたとしても，URL が不正ではないか，Web サイトのコンテンツが怪しくないか，ユーザが判断するように教育する．

3.1.2.2. URL **フィルタリング**

3.1.1.2 と同じ対策である．

3.1.2.3. EV **サーバ証明書が使用されていることの確認**

3.1.1.3 と同じ対策である．

3.1.2.4. **失効の確認**

ブラウザでサーバ証明書の失効を確認する．CA が，不正なサーバ証明書を発行したことに気づき，該当するサーバ証明書を失効させた場合は，ブラウザにおける証明書の失効確認の機能によりサーバ証明書が不正であることが分かる．但し，このためにはユーザが失効の確認を行うようにブラウザを設定する必要がある．

3.1.2.5. **信頼する証明書の更新**

攻撃により CA の運営自体が信頼できなくなった場合は，ブラウザベンダが，攻撃された CA の CA 証明書を，トラストストアの信頼する証明書から除外する更新を行う[10]．この更新はブラウザベンダによりブラウザのアップデートとして提供される．ユーザがこのアップデートを計算機に適用することにより，ブラウザは攻撃された CA の CA 証明書を信頼しなくなる．

3.2 マルウエアへの対策

3.2.1 自製サーバ証明書を使用したマルウエアへの対策

3.2.1.1. **ユーザの教育**

マルウエアと C&C サーバ間の SSL 通信においては，ユーザのインタラクトは入らないことから，対策として該当しない．

3.2.1.2. URL **フィルタリング**

3.1.1.2 と同様に，SSL 通信(HTTPS)に対して URL フィルタリングを実施することで，マルウエアによる C&C サーバへのアクセスを制限する．

3.2.1.3. EV **サーバ証明書が使用されていることの確認**

マルウエアと C&C サーバ間の SSL 通信においては，ユーザのインタラクトは入らないことから，対策として該当しない．

3.2.2 CA **を攻撃し入手した正規のサーバ証明書を使用したマルウエアへの対策**

3.2.2.1. **ユーザの教育**

3.2.1.1 に同じ．

3.2.2.2. URL **フィルタリング**

3.2.1.2 に同じ．

3.2.2.3. EV **サーバ証明書が使用されていることの確認**

3.2.1.3 に同じ．

3.2.2.4. **失効の確認**

マルウエアと C&C サーバ間の SSL 通信においては，ユーザのインタラクトは入らないことから，対策として該当しない．

3.2.2.5. **信頼する証明書の更新**

3.1.2.5 と同じ対策である．マルウエアが，サーバ証明書の検証に計算機におけるトラストストアの CA 証明書を参照する場合への対策である．

4. 不正なサーバ証明書を悪用した通信への提案する対策

企業や教育機関などの組織では，その組織のセキュリティ方針により，ユーザからアクセスを許可／禁止する Web サイトを統制できることが多い．その統制は情報システム部門が行う．このことを踏まえ，本章では組織が受け入れないサーバ証明書を検知することによる不正なサーバ証明書を悪用したフィッシングとマルウエアの通信への提案する対策を述べる．

4.1 フィッシングへの対策

4.1.1 自製サーバ証明書を使用したフィッシングへの対策

4.1.1.1. **組織が受け入れないサーバ証明書の検知**

図 3 において，本対策を実現する監視装置を示す．監視装置は情報システム部門が

Vol.2012-DPS-150 No.36
Vol.2012-CSEC-56 No.36
2012/3/1

運用する．
監視装置は，組織が信頼する CA の情報（証明書）を保持し，以下の処理を行う．
① 監視装置をスイッチなどのミラーポートに接続し，通信をモニタリングする．
② 監視装置は SSL のハンドシェイクを識別し，含まれるサーバ証明書を抽出する．
③ 抽出したサーバ証明書を組織において信頼する CA 証明書で検証[1]する．
④ 検証に成功した場合は，通信のモニタリングを継続する．
⑤ 検証に失敗した場合は，不正なサーバ証明書を検知したと判断し，そのサーバ証明書を用いた暗号化通信を行っている計算機を特定し，その計算機のユーザに対して警告を行う（その計算機を使用しているユーザへ警告メールを送信するなど）．

③においては，有効期限，拡張，失効状態まで検証することが望ましいが，そもそも，自製サーバ証明書は，組織が信頼する CA 証明書の秘密鍵で署名されているわけではないため，パスの構築と署名の検証のみでも効果があると考える．
2.1.2 に示した方法により，ユーザの計算機において，攻撃者の自製 CA 証明書がトラストストアにインストールされ信頼されている場合は，ブラウザは自製サーバ証明書の検証に成功する．従って，ユーザは不正な Web サイトであることに気がつかない．一方で，監視装置においては組織が信頼する CA 証明書のみが保持されているため，自製サーバ証明書の検証には失敗するので，組織が受け入れない証明書が流入していることが分かる（図 4）．

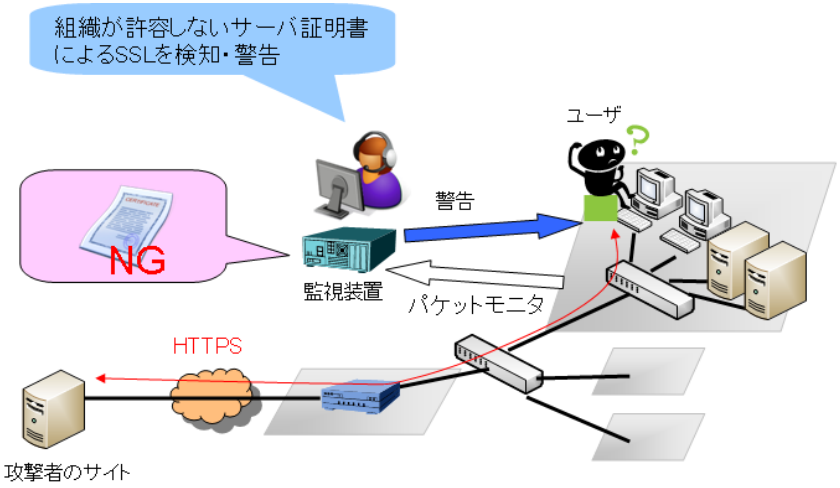

図 3 組織が受け入れないサーバ証明書の検知による対策

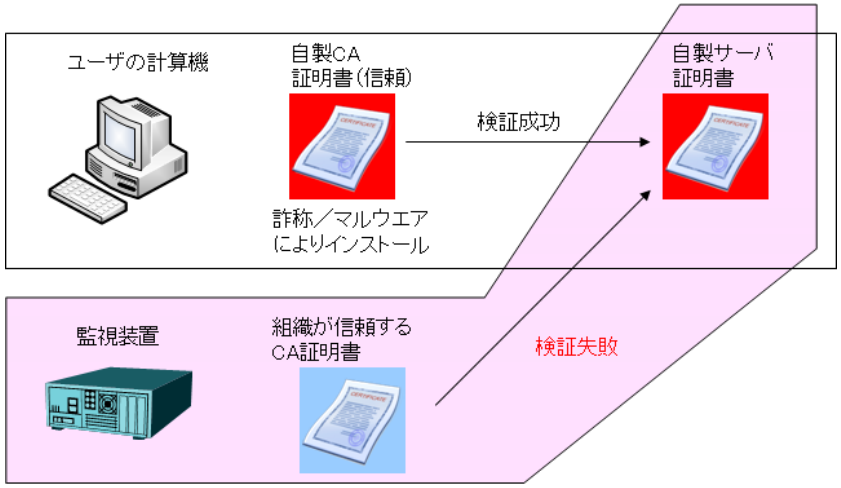

図 4 監視装置によるサーバ証明書の検証

4.1.2 CA を攻撃し入手した正規のサーバ証明書を使用したフィッシングへの対策

4.1.2.1. 組織が受け入れないサーバ証明書の検知

4.1.1.1 と同じ対策である．CA により該当するサーバ証明書が失効されている場合においては，監視装置における証明書の検証において，失効の確認を行うことにより，サーバ証明書が不正であることを検知できる．

攻撃により CA の運営自体が信頼できなくなった場合は，CA への攻撃について情報公開されたタイミングで，監視装置が保持している「組織が信頼する証明書」から，該当する CA 証明書を除外することで，該当する CA が発行したサーバ証明書の検証に失敗するため，このサーバ証明書が不正であることを検知できる．

4.2 マルウエアへの対策

4.2.1 自製サーバ証明書を使用したマルウエアへの対策

4.2.1.1. 組織が受け入れないサーバ証明書の検知

4.1.1.1 と同じ対策である．C&C サーバが使用する SSL のサーバ証明書が自製である場合，監視装置において「組織が信頼する CA 証明書」によるサーバ証明書の検証に失敗するため，サーバ証明書が不正であることが分かる．

4.2.2 CA を攻撃し入手した正規のサーバ証明書を使用したマルウエアへの対策

4.2.2.1. 組織が受け入れないサーバ証明書の検知

4.1.2.1 と同じ対策である．

Vol.2012-DPS-150 No.36
Vol.2012-CSEC-56 No.36
2012/3/1

5. 不正なサーバ証明書を悪用した通信への対策についての考察

表 1に不正なサーバ証明書を用いたSSL通信への従来の対策と提案する対策についてまとめ，考察する．

5.1 フィッシングへの対策についての考察

5.1.1 従来の対策

5.1.1.1. ユーザの教育

自製 CA 証明書がユーザの計算機のトラストストアにインストールされていない状態では，フィッシングサイトに接続するとブラウザが証明書の警告を表示するため，ユーザの教育は自製サーバ証明書への対策として有効と考える．自製 CA 証明書がトラストストアにインストールされている状態，及び，CA への攻撃により不正発行された正規サーバ証明書が設定されたフィッシングサイトへの接続においては，ブラウザは証明書についての警告を表示しない．そのため，3.1.1.1 に述べたように，ユーザは，ブラウザの警告無しに接続された SSL 対応 Web サイトの怪しさを判断する指針を示したマニュアルを参照する必要がある．しかし，ユーザがうっかり注意を怠ったり，判断を誤る可能性があり，判断はユーザに依存するため組織全体への対策としての効果は期待できない．

5.1.1.2. URL フィルタリング

ホワイトリストによる接続先の制限では，その作り方によりアクセス可能な Web サイトが限られ，企業では業務に支障をきたす場合がある．また，ブラックリストによる制限では，その作り方により，不正な Web サイトが漏れる可能性がある．URL の怪しさの度合いを判定するレピュテーション方式もあるが，完全ではない．

しかしながら，フィルタリングするリストが適切に作成されれば，URL フィルタリングは，自製 CA 証明書がトラストストアにインストールされていない場合とされている場合の両方及び，不正発行された正規サーバ証明書への対策として有効である．不正発行された正規サーバ証明書を用いるフィッシングサイトの URL が，ホワイトリストに記載されていなければ，CA が攻撃されサーバ証明書が発行されたことが判明する前においても，フィッシングサイトへの接続をフィルタする可能性がある．

5.1.1.3. EV サーバ証明書が使用されていることの確認

[8][9]によれば，EV サーバ証明書の判断は，特定のポリシーID が Certificate Policies 拡張に設定されていることの確認で行われる．従って，本稿で課題とするような自製の CA 証明書をトラストストアにインストールする攻撃の場合，EV サーバ証明書を自製することも可能と考えられる[8][9]．また，CA が攻撃され，EV サーバ証明書が不正に発行される可能性もある．従って，Web サイトに接続した際に，ブラウザの表示が EV サーバ証明書を示していることだけでは，その Web サイトがフィッシングサイトではないと断定できない．

5.1.1.4. 失効の確認

不正発行された正規サーバ証明書に対して，攻撃された CA がこの証明書を失効させた場合のみ対策として有効である．CA が攻撃された事実が判明し，失効が実施されるまでの間，本対策は無効である．

5.1.1.5. 信頼する証明書の更新

不正発行された正規サーバ証明書については，CA が攻撃されたことを情報公開するタイミングに対し，ブラウザのアップデートの提供が遅れる場合や，ユーザがブラウザのアップデートを計算機に適用するまでの間は，ブラウザはサーバ証明書が不正であることを判定できない．CA が攻撃され不正に正規サーバ証明書が発行されたことが判明する前は，ブラウザベンダは当対策を実施することができない．

表 1　不正なサーバ証明書を用いた通信への対策

対策＼不正な証明書		不正なサーバ証明書を悪用したフィッシング			不正なサーバ証明書を悪用したマルウエア	
		自製サーバ証明書		不正発行された正規サーバ証明書	自製サーバ証明書	不正発行された正規サーバ証明書
		自製 CA 証明書 TS 無し※1	自製 CA 証明書 TS 有り※2			
従来	ユーザの教育	○	×	×	—	—
	URL フィルタリング	△	△	△	△	△
	EV サーバ証明書が使用されていることの確認	○	×	×	—	—
	失効の確認	—	—	△	—	—
	信頼する証明書の更新	—	—	△	—	△
提案	組織が受け入れないサーバ証明書の検知	○	○	△	○	△

○：有効，△：状況により有効，×：無効，—：該当しない
※1 自製 CA 証明書の TS（Trust Store：トラストストア)へのインストール無し．
※2 自製 CA 証明書の TS（Trust Store：トラストストア)へのインストール有り．

Vol.2012-DPS-150 No.36
Vol.2012-CSEC-56 No.36
2012/3/1

5.1.2 提案する対策

5.1.2.1. 組織が受け入れないサーバ証明書の検知

自製 CA 証明書が，トラストストアにインストールされていない場合とインストールされている場合の両方において，対策として有効である．また，不正に発行された正規サーバ証明書については，CA が攻撃の事実を公表してから，ブラウザのアップデート適用により信頼する証明書の更新が計算機に反映されるまでの間，監視装置が保持している「組織が信頼する証明書」から，該当する CA 証明書を除外することで検知可能であるため，この証明書を用いたフィッシングによる被害を低減できる．

5.1.3 結論

自製 CA 証明書が，ユーザの計算機におけるトラストストアにインストールされていない場合とされている場合の両方に対して有効であること，さらに，不正発行された正規サーバ証明書に対して，CA が攻撃の事実を公表した時点で対策できることから，提案する対策が SSL に対応したフィッシングへの対策として有効であると判断する．提案する対策では，不正発行された正規サーバ証明書に対して，CA が攻撃の事実を公表する前は，この証明書が不正であることを検知できない．CA が攻撃されてからその事実を公表するまでのフィッシング対策として，URL フィルタリングを併用することが考えられる．5.1.1.2 で述べたように，フィルタリングするリストに依存するが，フィッシングサイトへの接続をブロックできる可能性がある．

5.2 マルウエアへの対策についての考察

5.2.1 従来の対策

5.2.1.1. ユーザの教育

マルウエアと C&C サーバ間の SSL 通信においては，ユーザが関与しないため該当しない．

5.2.1.2. URL フィルタリング

5.1.1.2 と同様に，フィルタリングするリストが適切に作成されれば，自製サーバ証明書，及び，不正発行された正規サーバ証明書に対して，対策として有効である．

5.2.1.3. EV サーバ証明書が使用されていることの確認

マルウエアと C&C サーバ間の通信であり，ユーザが関与しないため該当しない．

5.2.1.4. 失効の確認

マルウエアと C&C サーバ間の通信であり，ユーザが関与しないため該当しない．

5.2.1.5. 信頼する証明書の更新

マルウエアが計算機におけるトラストストアの証明書を，サーバ証明書の検証のために参照している場合に限り，対策として有効である．

5.2.2 提案する対策

5.2.2.1. 組織が受け入れないサーバ証明書の検知

5.1.2.1 に同じである．

5.2.3 結論

5.1.3 と同じ理由で, 提案する対策と URL フィルタの併用が有効であると判断する．

6. おわりに

組織において，不正なサーバ証明書を悪用したフィッシング及びマルウエアの SSL 通信(HTTPS)への対策について考察した．不正なサーバ証明書は，攻撃者が自製する場合と，CA を攻撃して入手する場合がある．

いずれの場合も, 組織が受け入れないサーバ証明書の検知と URL フィルタの併用が有効であると判断した．また，組織が受け入れないサーバ証明書の検知は，証明書が抽出可能な他のアプリケーションの通信に対しても適用可能である．しかしながら，通信から証明書を抽出できないようなアプリケーションについては検知ができない．通信から証明書を抽出できない場合への対策として，ユーザの計算機のトラストストアの内容を組織の管理者が監査し，組織が許容する証明書のみが保存されるようにチェックする方法が考えられるため，今後の検討としたい．

参考文献

1) SSL and TLS, E.Rescorla, Addison Wesley
2) IPA テクニカルウォッチ『暗号をめぐる最近の話題』に関するレポート ～ SSL/TLS や暗号世代交代に関連する話題から ～, 2011 年 5 月,IPA http://www.ipa.go.jp/about/technicalwatch/20110511.html
3) About EV SSL Certificates http://www.cabforum.org/certificates.html#
4) http://www.microsoft.com/security/portal/ , Trojan:WinREG/Gowfi.A
5) 「新しいタイプの攻撃」の対策に向けた設計・運用ガイド 改訂第 2 版，IPA
6) 不正な電子証明書発行に関する問題について, 2011 年 9 月,IPA, http://www.ipa.go.jp/security/ciadr/vul/20110915-sslcert.html
7) Phishers Experiment with Fake SSL Certificates http://news.softpedia.com/news/Phishing-Attacks-Move-to-Using-Fake-SSL-Certificates-186445.shtml
8) Faking Extended Validation SSL Certificates in Internet Explorer 7 June 7th 2007, V1.1 http://www.keyon.ch/de/index.php
9) Testing the limits of EV certificates,Simon Blanchet, et al, DEFCON SWITZERLAND 2010 (Presentation Slide) https://www.hashdays.ch/assets/files/slides/oechslin_testing_the_limits_of_ev_certificates.pdf
10) 【1】不正な SSL 証明書による問題, JPCERT/CC WEEKLY REPORT 2011-09-07 http://www.jpcert.or.jp/wr/2011/wr113401.html