NTTデータ先端技術のセキュリティ

NTT DATA
Trusted Global Innovator

INTELLILINK セキュリティ情報配信サービス
注目されているセキュリティ事故・事件に関する情報
＜2022年6月版 (第41号)＞ (選り抜き版)

2022年6月28日
ＮＴＴデータ先端技術株式会社
サイバーセキュリティ事業本部

今回のサマリー

証明書の発行ログを悪用した攻撃とその原因

WebサイトのHTTPS化が進む昨今、日々数多くの証明書が発行されています。一方、証明書発行の仕組みのうち、「証明書の透明性(CT: Certificate Transparency)」が攻撃対象のサーバを探索する手段の一つとして、攻撃者に悪用されています。なぜCTの仕組みが探索手段の一つとなり得るのか、その原因と対策について解説します。

証明書の発行ログを悪用した攻撃とその原因

1. 証明書の透明性(CT: Certificate Transparency)とは (1/2)

証明書の透明性(CT: Certificate Transparency)は、認証局による証明書の誤発行や、悪意のある攻撃者などによる不正な証明書の発行を検知する仕組みです。

＜登場の背景＞

この仕組みの登場の背景は、「認証局への信頼が薄れる事態があった」ためです。そもそも、証明書の信頼性は、その証明書を発行した認証局の信頼に基づいています。このため、信頼済みの認証局が何らかの理由で不正な証明書を発行してしまった場合、その証明書は正規のものと見分けがつかなくなります。

実際に、認証局が攻撃者により不正アクセスを受けたり、認証局の不手際で不正に証明書を発行した事例があります(※1,2)。

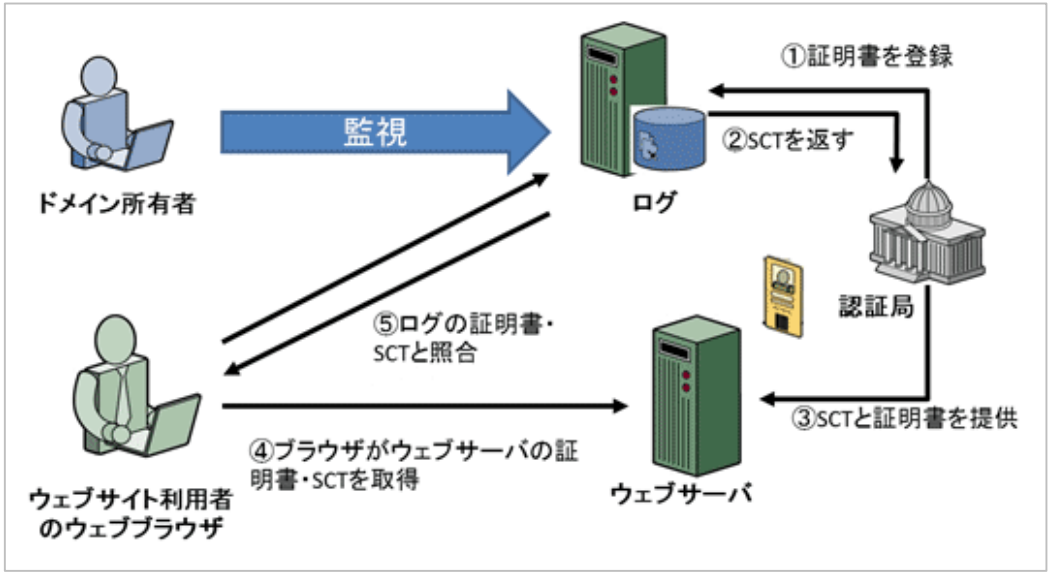
このような認証局の行動に不正がないかを監視する目的で作られた仕組みがCTです。

※1 DigiNotarの不正証明書問題、その影響は – @IT
https://atmarkit.itmedia.co.jp/news/201109/08/diginotar.html
※2 Symantecの証明書発行に不手際、Googleが対応を要求 - ITmedia エンタープライズ
https://www.itmedia.co.jp/enterprise/articles/1510/30/news061.html

1. 証明書の透明性(CT: Certificate Transparency)とは (2/2)

＜仕組みの概要＞

　CTでは、認証局が証明書を発行する際に、証明書を「CTログ」に登録(※)し、登録後に得られる「Signed Certificate Timestamp (SCT)」と呼ばれる署名を付与した証明書を認証局が発行します。ドメイン管理者やWebサイト利用者はこのSCTをもとにCTログを調べることで、証明書が不正に発行されたかを確認することができます。



引用: Certificate Transparency(証明書の透明性)| DigiCert
https://www.websecurity.digicert.com/ja/jp/theme/ssl-certificate-transparency?id=ssl-certificate-transparency

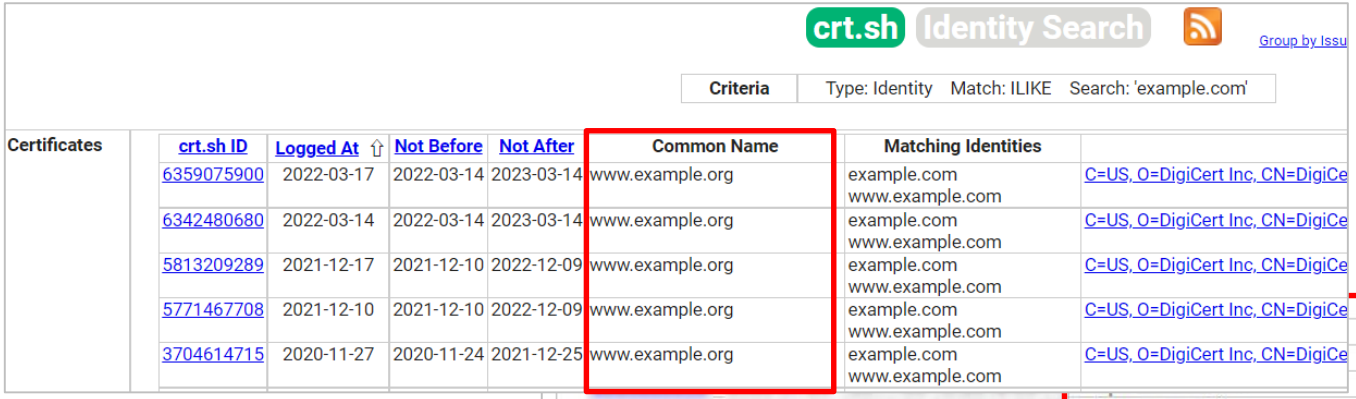
※近年は証明書のCTログへの登録がデフォルトになりつつあります。
　なお、認証局によっては、証明書のCTログへの登録を行わないようにする(CTの仕組みを用いない)オプションもあります。

2. CTログからわかること

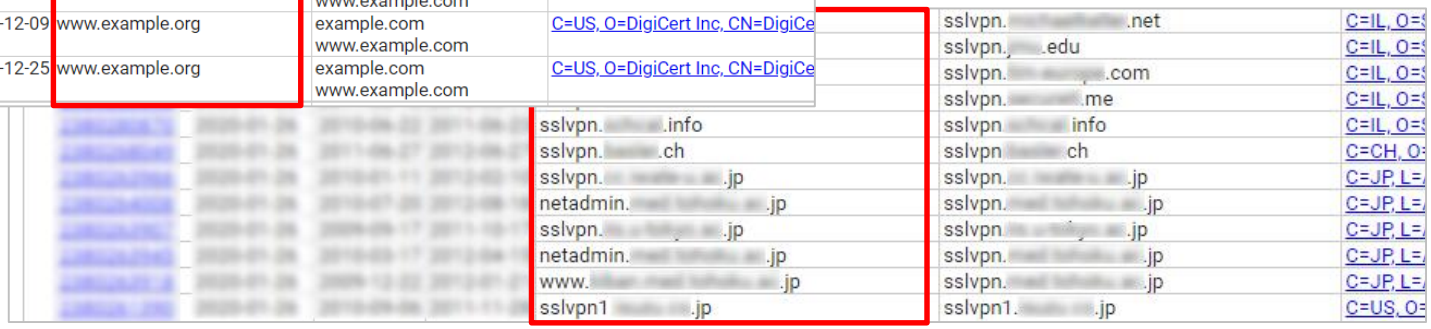
　前述の通り、ドメイン管理者やWebサイト利用者はCTログを調べることで、証明書が不正に発行されたかを確認することができます。

　一方で、CTログに記録された証明書の情報(コモンネーム)から、サーバに設定されたFQDNを特定することもできます。これにより、一般には公表していない/したくないFQDNが証明書から明らかになることがあります。

　実際に、「crt.sh」など、CTログを検索するサービスを用いることで、誰もが簡単に過去の証明書発行履歴やFQDNを確認することができます。



「examle.com」上で稼働していると推測されるホスト



VPN関連の製品が稼働していると推測されるホスト

3. CTログの悪用事例

脆弱なサーバを「探す」手段の一つとして、攻撃者はCTログを定期的/リアルタイムで監視し、CTログから得られたFQDNをもとに攻撃を仕掛ける場合があります。

FQDNにはサーバの用途を特徴づける文字列が含まれている場合が多く、特に「test」「dev」といった文字列がある開発/検証用サーバは、本番サーバと比較すると、一時的な設定不備や管理漏れにより攻撃が成功する可能性が高くなります。また、「vpn」のようなリモートアクセス系サーバは組織のネットワークへの侵入口として攻撃対象になりやすくなります。

Let's Encryptのコミュニティサイトでは、「構築中のWordPressサーバが証明書発行からすぐに攻撃された」という投稿があります。投稿者曰く、「攻撃対象をCTログから探し出している」とのことで、乗っ取られたサーバはDDoS攻撃に悪用されました。

Hacked new wordpress sites, because LE is created

Help

raj — Apr 6

Hello,

we found more sites, which was hacked very fastly after LE generated.
Our clients start installation after LE was green, but in meantime (max 15 minutes after LE) robot from 185.59.221.* come and use WP installation files to prepare hack. Days after - on all domain call malware script and start DDOS to IP from France. I think that it is because crt.sh is scanned.

Here info too: Unknown file in WordPress core: wp-includes/.query.php | WordPress.org 39

Malware script was wp-includes/.query.php

Any idea what with this?🙂

Pavel

引用：Hacked new wordpress sites, because LE is created
https://community.letsencrypt.org/t/hacked-new-wordpress-sites-because-le-is-created/175284

4. CTの必要性と影響の緩和策

証明書発行の際にCTの仕組みが用いられることで、CTログから「一般には公表していない/したくないFQDNが証明書から明らかになる」というリスクは存在しますが、基本的には以下の理由からCTの仕組みは用いられるべきです。

- 本来の目的が、不正な証明書の発行を検知する仕組みであること
- ブラウザによっては証明書エラーとなる場合があること(※1,2)
- FQDNが明らかになったことが攻撃成功に直結するわけではない(標的サーバを探す手法の一つに留まる)こと(次ページ参照)

なお、ワイルドカード証明書を発行することで、CTの仕組みが用いられた場合でも、ホストを特定できるようなFQDNが晒されるリスクはなくなります。

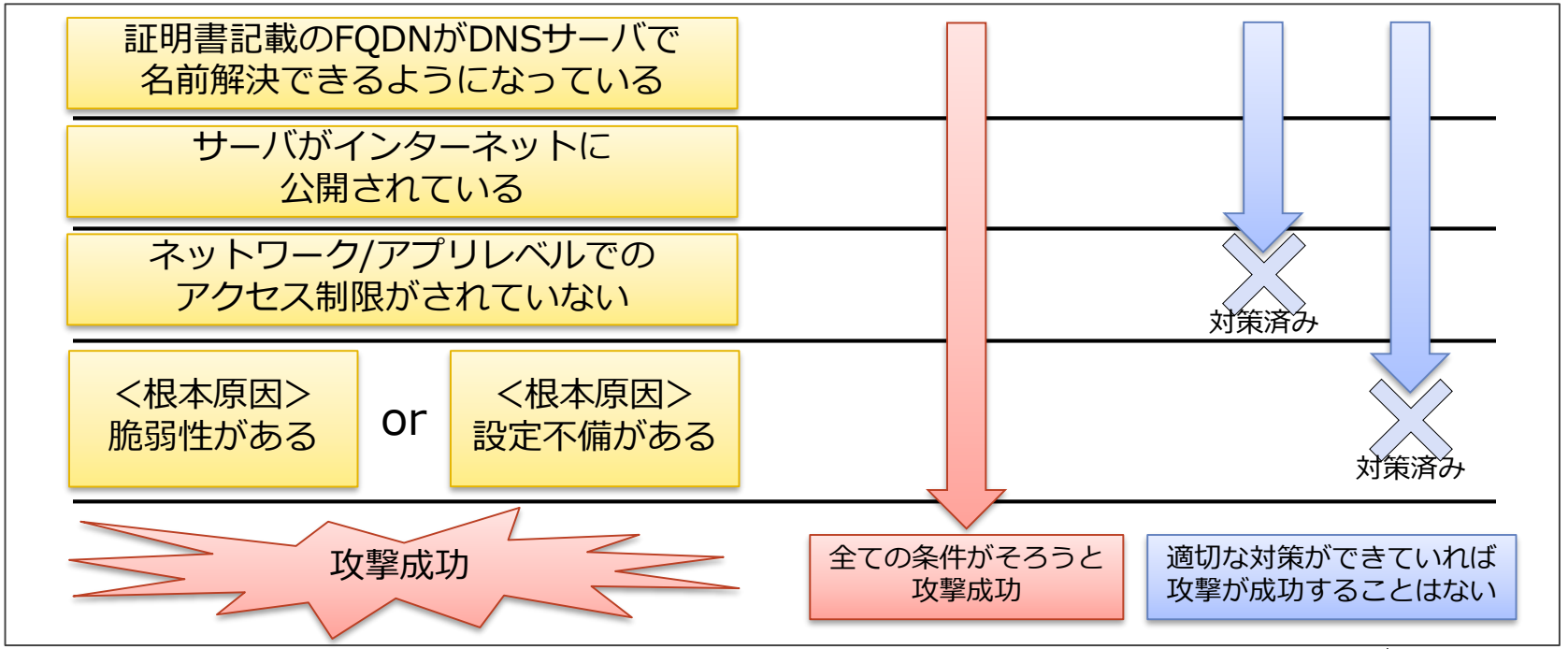
また、認証局によっては、証明書のCTログへの登録を無効化して証明書の発行ができます。社内系システムの証明書など、インターネットに公開予定のないサーバであれば効果的です。

※1 Certificate Transparency
https://chromium.googlesource.com/chromium/src/+/master/net/docs/certificate-transparency.md
※2 Certificate Transparency(証明書の透明性)| DigiCert
https://www.websecurity.digicert.com/ja/jp/theme/ssl-certificate-transparency?id=ssl-certificate-transparency

5. 被害に遭うそもそもの原因

証明書の発行により、一般には公表していない/したくないFQDNが証明書から明らかになった場合でも、対象のサーバですぐに攻撃が成功するわけではありません。攻撃が成功する原因は、サーバ上で脆弱性のある製品の稼働や、サーバ/製品の設定不備にあります。更に、このような脆弱なサーバがインターネットからアクセスできるような状態になっている場合に、初めて被害に遭う可能性が発生します。

したがって、根本原因が適切に対策されていれば、証明書を発行したり、インターネットに公開したりしても問題はありません。



6. 対策

システムを運用している組織においては、設計段階で個々のサーバがインターネットから直接アクセスできる必要性を検討するとともに、運用中のサーバについては漏れなく存在と構成を掌握し、各サーバで稼働するサービスの管理を行うことが大切です。また、脆弱性の公開時や万が一のインシデントに備えた体制/手順の確認も大切です。

- **サーバがインターネットから直接アクセスできる必要性の再確認**
  システム全体の設計段階から、各種サーバをインターネットからアクセス可能な位置に配置しないで済むよう検討してください。インターネットからのアクセスが必須な場合は、必要最小限のアクセスとするために、ネットワークやサーバでアクセス制御を行ってください。
- **システムで利用しているサーバやソフトウェアなどの把握/最新化**
  脆弱性の対策として最新化は最も効果的ですが、そのためには対象機器を把握しておく必要があります。特に、ネットワーク機器、サーバ機器、アプライアンス製品は、運用者やユーザが日常的に操作するものではないため、その存在を意識しておく必要があります。また、保守契約やEOLも確認し、常に最新化できる状態であるかを確認してください。
- **システムが持つサービスの公開状況の可視化と診断**
  システムが持つ全てのグローバルIPアドレスやFQDNに対して、ネットワークスキャナや外部の検索サービスを用いてサービスの公開状況や応答を確認し、意図していないサービスが公開されていないかを攻撃者視点で確認してください。あわせて、ネットワーク診断により公開中のサービスの脆弱性有無を確認してください。
- **一時的なシステムの秘匿や停止に関する体制や手順の確認**
  深刻な脆弱性が公開されたり、万が一攻撃により侵害を受けたりした場合を想定して、体制や手順を確認してください。

7. まとめ

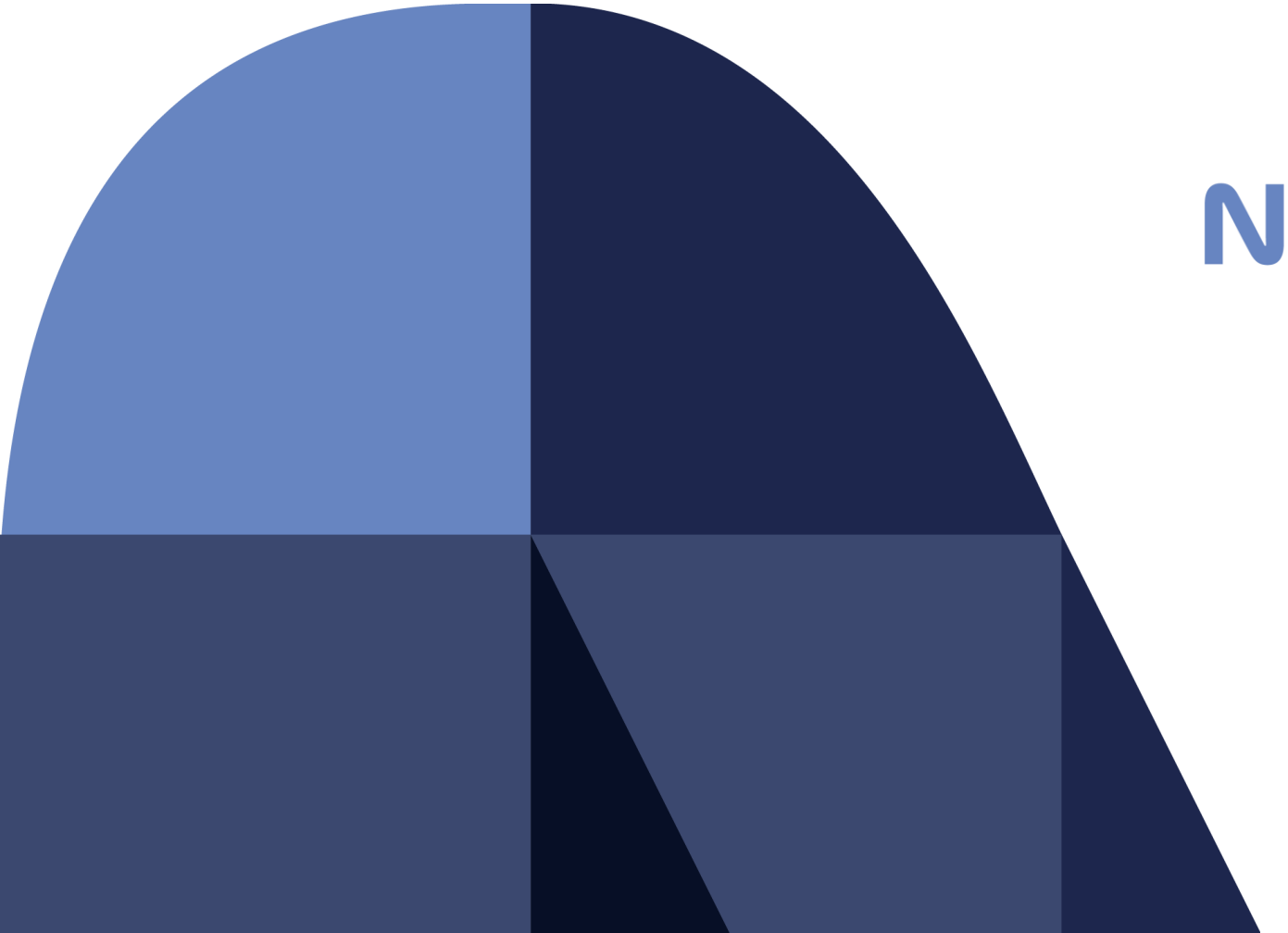
本記事では、証明書の発行ログを悪用した攻撃とその原因について解説しました。

CTは、認証局の行動に不正がないかを監視する目的で作られた仕組みです。一方で、攻撃対象のサーバを探索する手段の一つとして、攻撃者はこの仕組みを悪用し、証明書の発行ログ(CTログ)から攻撃対象のサーバをリスト化していると推測されます。実際に、CTログの悪用で見つかったと推測されるサーバへの攻撃も確認されました。しかし、そもそも被害に遭う原因はサーバ上での脆弱性のある製品の稼働やサーバ/製品の設定不備であることに加え、このような脆弱なサーバをインターネットからアクセスできる状態にしているためです。

CTログが標的探索に悪用されていることを念頭に、システムを運用している組織においては、設計段階で個々のサーバがインターネットから直接アクセスできる必要性を検討するとともに、運用中のサーバについては漏れなく存在と構成を掌握し、各サーバで稼働するサービスの管理を行うことが大切です。また、脆弱性の公開時や万が一のインシデントに備えた体制/手順の確認も大切です。

8. 参考URL

- インターネット用語1分解説～Certificate Transparency (CT)とは～ - JPNIC
  https://www.nic.ad.jp/ja/basics/terms/ct.html
- Certificate Transparency
  https://chromium.googlesource.com/chromium/src/+/master/net/docs/certificate-transparency.md
- Certificate Transparency(証明書の透明性)| DigiCert
  https://www.websecurity.digicert.com/ja/jp/theme/ssl-certificate-transparency?id=ssl-certificate-transparency
- crt.sh | Certificate Search
  https://crt.sh/
- DigiNotarの不正証明書問題、その影響は – @IT
  https://atmarkit.itmedia.co.jp/news/201109/08/diginotar.html
- Symantecの証明書発行に不手際、Googleが対応を要求 - ITmedia エンタープライズ
  https://www.itmedia.co.jp/enterprise/articles/1510/30/news061.html
- Hacked new wordpress sites, because LE is created
  https://community.letsencrypt.org/t/hacked-new-wordpress-sites-because-le-is-created/175284
- WordPress sites getting hacked ‘within seconds’ of TLS certificates being issued | The Daily Swig
  https://portswigger.net/daily-swig/wordpress-sites-getting-hacked-within-seconds-of-tls-certificates-being-issued



NTT DATA

Trusted Global Innovator