経済産業省
Ministry of Economy, Trade and Industry

産業界へのメッセージ

令和２年４月１７日

産業サイバーセキュリティ研究会

産業界へのメッセージ①

- 攻撃の痕跡を発見しにくいファイルレスマルウェアの利用など**攻撃の高度化**、海外事業所や取引先企業を通じた侵入経路の確立など**攻撃起点の変化・拡大**への対応が必要に。
- 直近、新型コロナウィルスの混乱に乗じて、**ランサムウェアや不正アプリ等の攻撃**も海外を中心に急増。
- 今般の事態を受け、今後、更にデジタル化を推進していくことの必要性が明らかになる中、改めてITシステムや制御システムの**セキュリティ対策の徹底と強化**をお願いしたい。

直近の状況に対応するために取り組んでいただきたいこと

- **新型コロナウィルスを騙る不正アプリや詐欺サイト、フィッシングメール/SMSに注意**すること。
- 上記の取組を効果的に進めるため、**NISCや、IPA、JPCERT等の専門機関からの注意喚起(※)を定期的に確認**すること。
- 機器・システムに対して、**アップデート等の基本的な対策**をできるだけ実施すること（利用環境に依存することに留意）。
- 可能な環境であれば、ランサムウェアに感染した事態に備えて**システムやデータのバックアップと復旧手順を確認**すること。

(※)4ページを参照のこと

産業界へのメッセージ②

デジタル化を進めていく中で取組を進めていただきたいこと

1 事前対策の確認・強化

- **サプライチェーン全体を視野に入れたリスク管理**を行うこと。
- 稼働中の機器・システムに対して、**サポート切れのOSやアプリは使用せず**、**パッチ当て等の基本的に求められる対策**（※）を実施することに加え、**振る舞い検知**など、既存の対策を**すり抜けた攻撃を防御・検知する仕組み**を導入すること。
- テレワークなど企業の管理策が及ばない起点や防御レベルが低い拠点からの侵入被害を限定するために、**情報資産やネットワークへのアクセスの継続監視と強化**、**システムの階層化**や、**子会社・海外拠点を含めた対応体制の整備**をすること。

（※）7ページ以降の「具体的な対策に関する参考情報」を参照のこと

2 事後対策の強化確認

- 攻撃されることを想定して、適切な**初動対応を行う体制と計画を整備**すること。
- インシデント発生時には、混乱した社員等の不適切な行動がセキュリティリスクを高めることも。平時の**“防災訓練”を徹底**して行うこと。

専門機関等からの注意喚起

参考1

内閣サイバーセキュリティセンター（NISC)

注意喚起情報　　https://twitter.com/nisc_forecast

直近発出された注意：テレワークを実施する際にセキュリティ上留意すべき点について
（令和２年４月14日）
https://www.nisc.go.jp/active/general/pdf/telework20200414.pdf

独立行政法人情報処理推進機構（IPA）

セキュリティ関連情報サイト：　　https://www.ipa.go.jp/security/

直近発出された注意：Zoomの脆弱性対策について（令和２年４月３日）
https://www.ipa.go.jp/security/ciadr/vul/alert20200403.html

情報セキュリティ安心相談窓口（※ 現在は新型コロナウィルスの感染拡大防止等のため、メールのみでの対応）
https://www.ipa.go.jp/security/anshin/　　メール： anshin@ipa.go.jp

その他（届出・相談・情報提供）　窓口一覧
https://www.ipa.go.jp/security/outline/todoke-top-j.html

JPCERT/CC (Japan Computer Emergency Response Team Coordination Center)

注意喚起サイト：　https://www.jpcert.or.jp/at/2020.html

直近発出された注意：長期休暇に備えて（令和２年４月14日）
https://www.jpcert.or.jp/newsflash/2020041401.html

インシデントの対応依頼（受け付けることのできる内容を確認し、メールにてご依頼ください）
https://www.jpcert.or.jp/form/　　メール：info@jpcert.or.jp

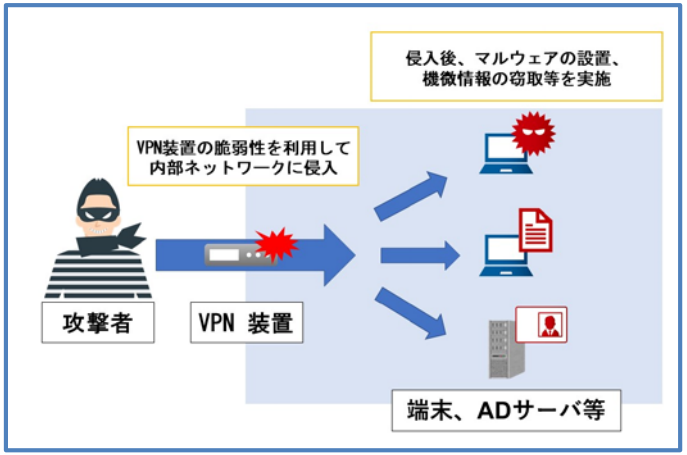
（追加参考情報）長期休暇に備えてーJPCERT/CCが4月14日に注意喚起

- 2020年4月14日、JPCERT/CCは、ゴールデンウィークの長期休暇期間におけるコンピュータセキュリティインシデント発生の予防および緊急時の対応に関して、要点を公表。
- 新型コロナウイルス感染症(COVID-19)の拡大に伴うテレワークの増加により、テレワーク環境の脆弱性等を起因とした攻撃への注意が必要。

■テレワーク環境の脆弱性等を起因とした攻撃

- JPCERT/CC では、VPN 製品である Citrix Application Delivery Controller および Citrix Gateway の脆弱性 (CVE-2019-19781) などについて、日本国内で脆弱性を悪用したと思われる攻撃が行われていることを確認。**遠隔の第三者が任意のコードを実行する可能性**。

・複数の Citrix 製品の脆弱性 (CVE-2019-19781) に関する注意喚起
https://www.jpcert.or.jp/at/2020/at200003.html
・Pulse Connect Secure の脆弱性を狙った攻撃事案
https://blogs.jpcert.or.jp/ja/2020/03/pulse-connect-secure.html



対策

■システム管理者・経営者における対策や対応

1. VPN 製品や FW を含めた自組織のシステムについて、アップデートの必要有無を確認する
2. 社内システムへのアクセス制御や認証方法を確認する
3. 利用サービスの攻撃事例やアップデート状況を確認し、利用継続を検討する

■個人・従業員における対策や対応

1. OSやウイルス対策ソフトを最新の状態に保つ
2. テレワーク用クライアントアプリ（テレビ会議、VPNアプリ）は正規のものをダウンロードする

出典：https://www.jpcert.or.jp/newsflash/2020041401.html
CyberNewsFlash：https://www.jpcert.or.jp/newsflash/

（追加参考情報）米CISAがTIC 3.0テレワークガイダンス暫定版を公表

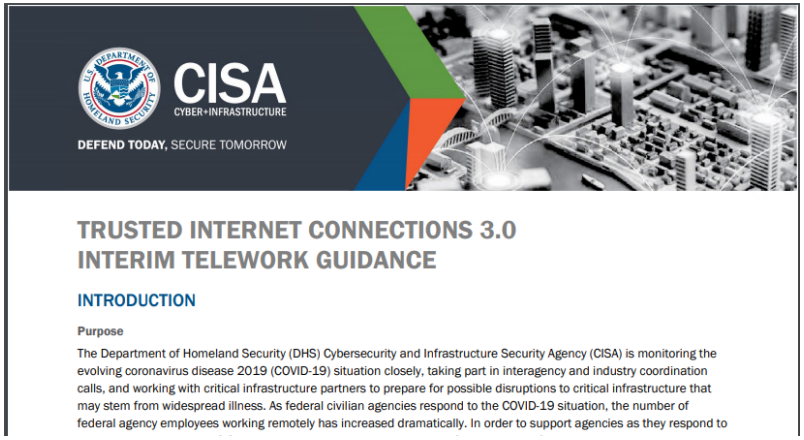
- 米CISAのTrusted Internet Connections(TIC)プログラム管理局が2020年4月8日、連邦政府機関職員向けのテレワークガイダンスの暫定版を公表。内容の一部は、現在ファイナル版作成中のTIC3.0関連ドキュメントに反映予定。

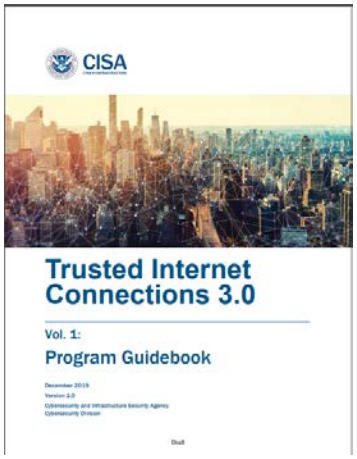
テレワークガイダンス暫定版の概要

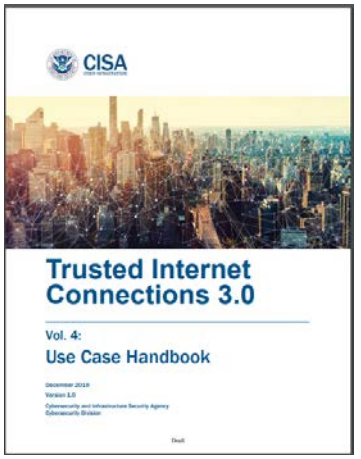
- 新型コロナウイルスの感染拡大に伴い、テレワークを実施する連邦政府職員が急増していることから、民間のネットワークやクラウド環境への安全な接続等、テレワーク関連の懸念に対処するための方策を示すもの。
- 本ガイダンスの一部は、今後公表予定のTIC 3.0 Remote User Use Caseに反映。

TIC 3.0について

- TICは連邦政府機関のインターネットアクセスの安全性向上等を目的に2007年に始まったイニシアチブ。
- 2019年12月、TIC3.0の関連ドキュメント（Program Guidebook、Reference Architecture、Security Capabilities Handbook、Use Case Handbook、Service Provider Overlay Hadbookの5部構成）を公表。パブリックコメント期間を経て、2020年春にファイナル版公表予定。







出典： https://www.cisa.gov/sites/default/files/publications/CISA-TIC-TIC%203.0%20Interim%20Telework%20Guidance-2020.04.08.pdf
https://www.cisa.gov/publication/tic-documents

参考2

業界横断的に対応が求められるサイバー脅威（脆弱性）の例

- **業界横断的に特に対応が求められる脅威**として、以下のものが考えられるところ。
- **どの脅威も基本的な対策により回避できるもの**であり、**各業界に本脅威情報と対策を周知することで、業界横断的なサイバーセキュリティ対策の底上げが期待**される。

要対応項目１：セキュリティパッチの適切な管理（Patching Cadence）

– ソフトウェアプログラムを更新し、修正や機能変更を行うための修正プログラムを適用すること。

要対応項目２：ネットワーク・認証の適切な管理（Network Security）

– ネットワーク外部からの不正アクセスを防止し、データの改ざんや情報漏えい、サービスの停止といったセキュリティ事案から情報資源を保護すること。

要対応項目３：DNSサーバ・レコードの適切な管理（DNS Health）

– 「IPアドレス」と「ドメイン名」を組み合わせて管理するシステム（DNS）について、なりすましや不適切な応答を行わないようにセキュリティを確保すること。

要対応項目４：アプリケーションの適切な管理（Application Security）

– アプリケーションに対する脅威からシステムを保護するため、アプリケーション内のセキュリティを確保すること。

詳細な説明と対策方法例は次ページから。

要対応項目１：セキュリティパッチの適切な管理（Patching Cadence）１

● Patching（パッチ当て）とは？　～不具合のあるソフトウェアの応急措置～

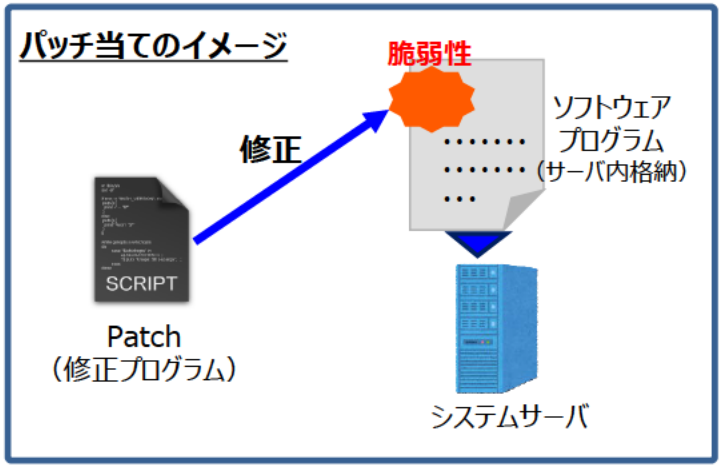
– ソフトウェアプログラムを更新し、修正や機能変更を行うための修正プログラムを適用すること。「パッチを当てる」と表現する。

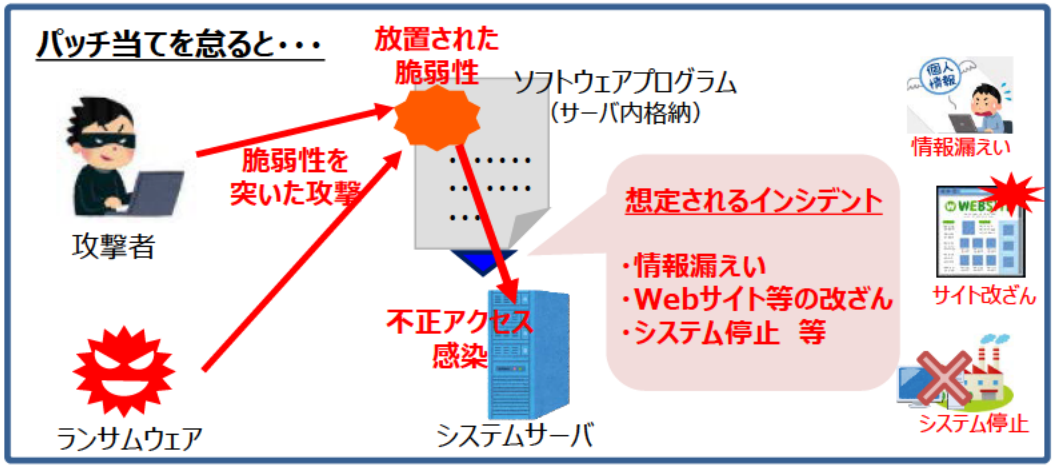
– ソフトウェアに脆弱性や問題点が発見された際などに、これらの不具合を解消するための手段として用いられる。

● Patching（パッチ当て）を怠ると？

– つまりはソフトウェアの脆弱性を放置していることに等しいので、あらゆるサイバー攻撃の温床となる。

– 想定されるサイバー攻撃被害は、不正アクセスによる情報漏えいやWebサイト等の改ざん、ランサムウェア感染によるシステム停止など、多岐に亘る。





要対応項目１：セキュリティパッチの適切な管理（Patching Cadence）２

● Patching（パッチ当て）はなぜ必要か？

– 近年のソフトウェアは、そのプログラムの複雑性から、脆弱性や問題点等の欠陥が存在することは避けられず、それは運用段階になってからも次々と発見される。

– 適時に適正なパッチ当てをすることで、システムの脆弱性の数を減らすことは、サイバーセキュリティ対策の基本。

● Patching（パッチ当て）の主な対策方法は？

– 最新の脆弱性情報を常に確認し、それに対応する最新のパッチを入手する手段を確立しておく。

– 普段から資産（ソフトウェア等）を把握し、パッチ当ての対象、時期、種類、バージョンを管理しておく。

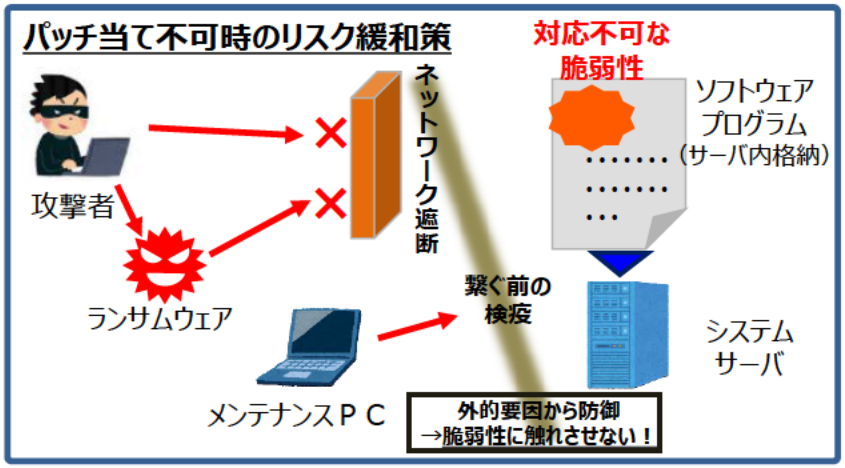
– 適切なパッチ管理のために、関連作業の手順化、スケジュール化などで業務の効率化を図る。

– パッチ当ては、OS（Windows/Linux）やアプリケーション、制御システムまであらゆるソフトウェアが対象

✓ システム（特に制御系）によっては、カスタマイズや独自で開発したソフトウェアの導入のため、パッチ当てがシステム全体に対して悪影響を及ぼすこともある。

✓ その場合、脆弱性放置によるリスクは許容せざるを得ないが、ネットワークからの遮断やメンテナンスPCの接続制限等、**リスク緩和策**を講じることが重要。

✓ 深刻な脆弱性の場合は、パッチを当てるまでサービスを停止させることを許容するなどの経営判断も必要。



要対応項目２：ネットワーク・認証の適切な管理（Network Security） 1

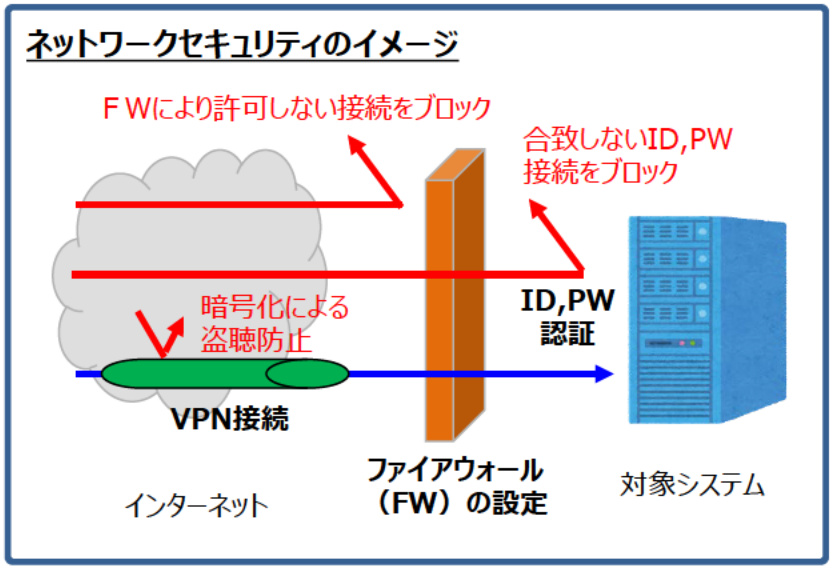
● Network Securityとは？ ～不正アクセスの防止～

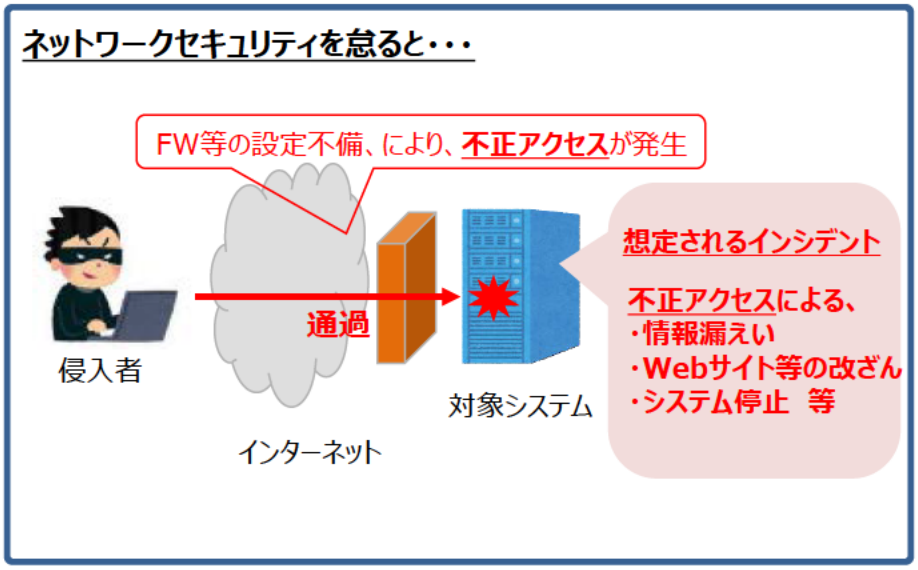
– 所有する情報資源（システム）をネットワークに接続して様々なサービスを利用する際、ネットワーク外部からの不正アクセスを防止し、データの改ざんや情報漏えい、サービスの停止といったセキュリティ事案から情報資源を保護すること。

● Network Securityを怠ると？

– システム利用の利便性向上にはネットワークへの接続は不可欠である一方、ネットワークセキュリティの不備による情報の漏えい等のセキュリティ事案が後を絶たない状況。

– 想定されるサイバー攻撃被害は、不正アクセスによる情報漏えいやWebサイト等の改ざんなど。





要対応項目２：ネットワーク・認証の適切な管理（Network Security） 2

● Network Securityの主な対策方法は？

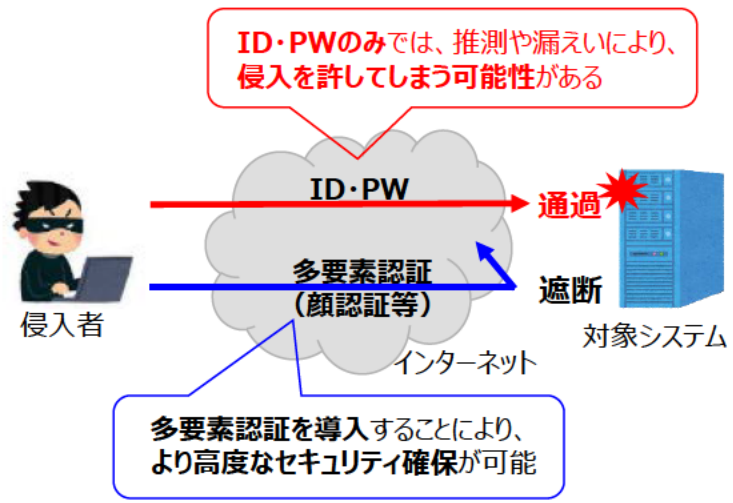
- ファイアウォール：ネットワークの外部と内部の境界に強固な壁を構築して、設定したルールに該当しない接続を防御する。
- アクセスコントロール：IPアドレスによる許可端末の確認や「ID」及び「パスワード」による認証などにより、適切な端末や利用者からの接続かどうかを判断し、不適切な接続をブロックし、制限する。
- VPN(Virtual Private Network)：端末とネットワーク間を暗号化して接続する。通信が暗号化されているため、仮に途中でインターセプト（盗聴）されても安全である。

✓ 近年、特にクラウドサービスの利用において、「ID」及び「パスワード」のみによる認証では、容易に推測できるパスワードを設定してしまうことや、使い回しされたパスワードの漏えい等により、不正ログインされてしまう事案が発生している。

✓ ひとたびクラウドサービスに不正ログインされると、内部や顧客とのメール、社内データの窃取、他組織への攻撃の踏み台とされる等、大きな被害に発展する可能性がある。

✓ そのため、ワンタイムパスワードや顔認証等の異なる要素を加えた認証（**多要素認証**）を導入することで、より高度なセキュリティを確保することが求められる。

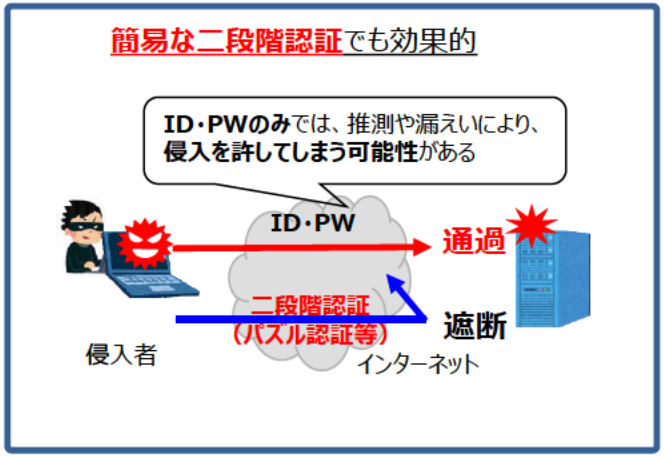
多要素認証の利点



要対応項目２：ネットワーク・認証の適切な管理（Network Security） 3

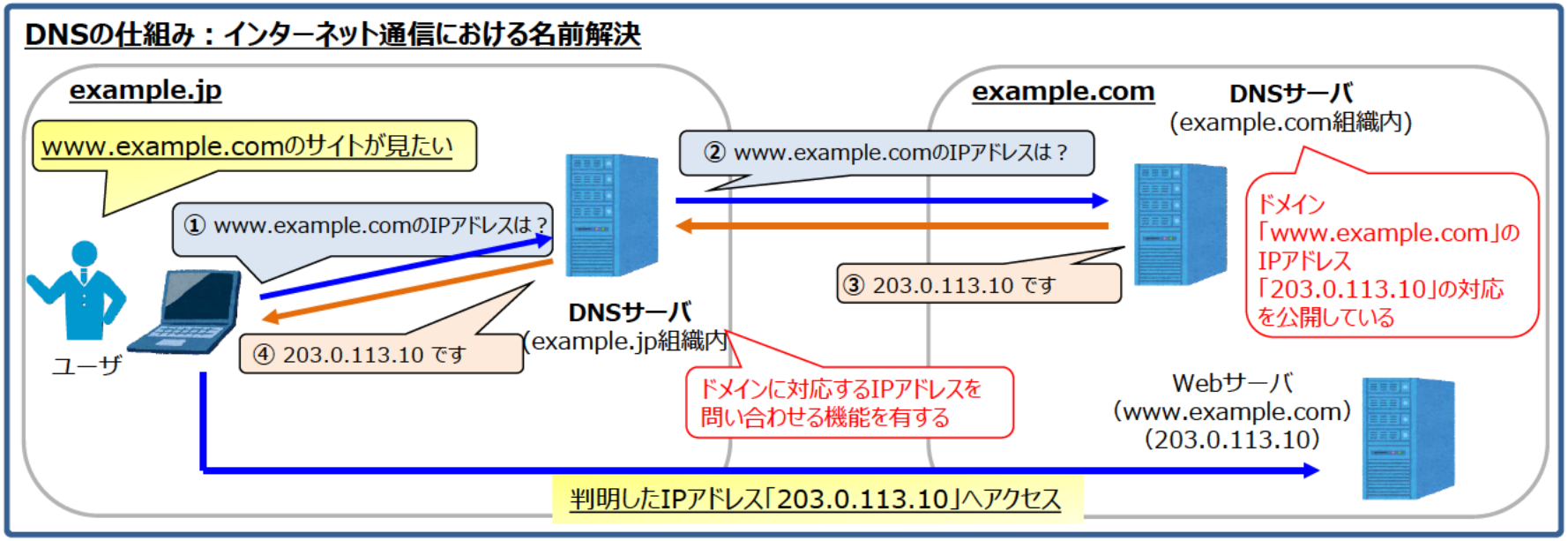
● 最近特に増加しているリスト型攻撃とその対処法は？

- 最近特に一般ユーザ向けのWebサイト（会員サービスサイトやショッピングサイト等）において、「ID」及び「パスワード」のみによる認証しか行っていない場合に、不正ログインされてしまう事案が多発している。
- 従来の「ブルートフォース攻撃/辞書攻撃」と呼ばれる、IDとパスワードを総当たりで試す攻撃は、１つのIDに対して大量のログイン試行と失敗が発生することから、検知が容易であった。
- しかし最近は、ユーザが複数のサービスで同じIDとパスワードを使いまわす習慣を狙い、他の事案で流出したIDとパスワードがセットとなったアカウント情報リストを利用した「リスト型攻撃」が増えてきている。リスト型攻撃は不正ログインの成功確率が高く、また１つのIDに対するログイン試行回数が少ないため、攻撃に気付きにくい。
- 攻撃はロボットプログラムで自動実行されることが多いので、手動動作を必要とするパズル認証を追加するなど簡易な二段階認証を導入することでも、より高度なセキュリティを確保が可能である。



要対応項目３：DNSサーバ・レコードの適切な管理（DNS Health） 1

- **DNS（Domain Name System）とは？　～「IPアドレス」と「ドメイン名」の管理～**
  - インターネット上で使用する「IPアドレス」と「ドメイン名」を組み合わせて管理するシステムのこと。
    - ✓ 「IPアドレス」は、インターネット上におけるコンピュータ独自の住所。「198.51.100.1」などと表記。
    - ✓ 「ドメイン名」は、IPアドレスが人間に判別できるように付した英数字の記号。「meti.go.jp」などと表記。
  - つまり、コンピュータがインターネット上で扱う「IPアドレス」と、人間の理解できる標記である「ドメイン名」のつなぎ役。インターネット通信において重要な役割を担っている。
  - 特に、メール送信元のドメイン名が詐称されていないかを検査するための仕組みであるSPFは、DNSのこの機能を利用している（詳細は次ページ）。



要対応項目３：DNSサーバ・レコードの適切な管理（DNS Health）２

● SPF（Sender Policy Framework）とは？　～なりすましメールの防止～

– メールのなりすまし防止やスパムメール対策の一つであり、送られてきたメールが、正規のメールサーバから送信されているかを判断するためのもの。

– 管理者がDNSサーバ（において公開しているSPFレコード）に、メールサーバの「ドメイン名」に対応する「IPアドレス」を記載しておくことで、メール受信者は、正規のメールサーバから送信されたメールかどうか確認できる。

● SPFを設定しないと？

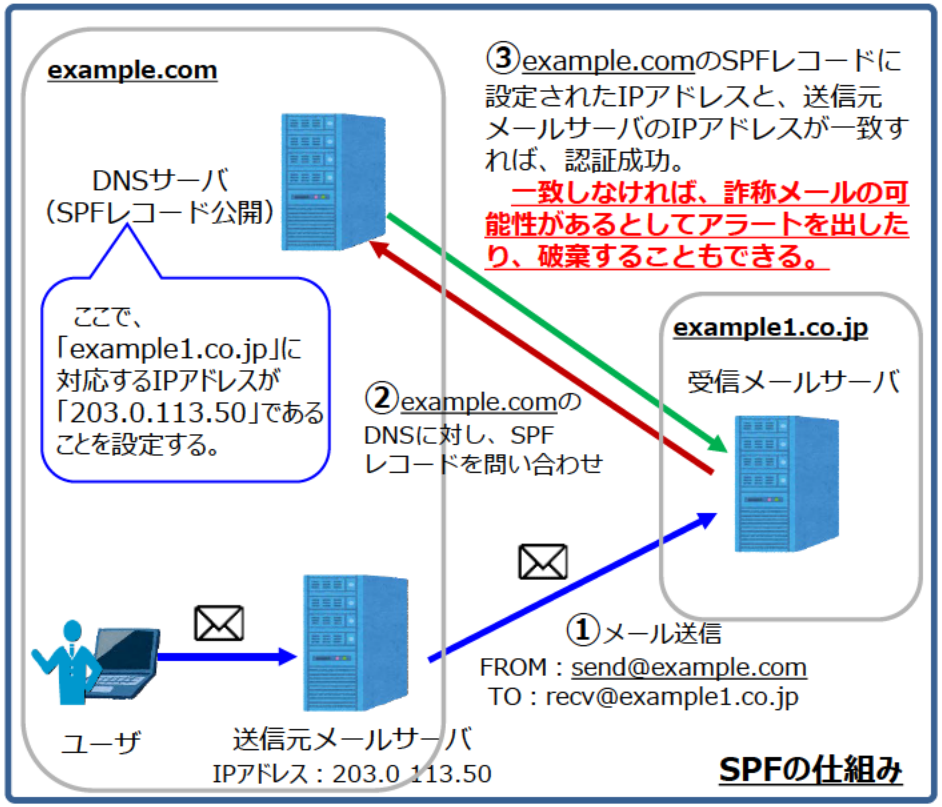
– 攻撃者は、送信元メールアドレスを貴方の組織に詐称し、「なりすましメール」を送付することで、受信者をだまそうとする。

● SPFを確認しないと？

– 「なりすましメール」の受信者は、信頼できる送信元からのメールであると信じてしまい、悪意のある添付ファイルやURLリンクを疑うことなく開き、感染してしまう可能性が高まる。

✓ より安全なメール環境の実現に向けて

- DKIM(DomainKeys Identified Mail)やDMARC (Domain-based Message Authentication, Reporting, and Conformance)といった認証技術がある。



要対応項目４：アプリケーションの適切な管理（Application Security） 1

● Application Securityとは？　～アプリケーションの保護～

– アプリケーション（ソフトウェアの一種で、使用者の業務に応じて作成したプログラム）に対する脅威からシステムを保護するため、アプリケーション内のセキュリティを確保すること。

– アプリケーションに対する脅威には、DoS攻撃や不正アクセスによる情報漏えいやデータ改ざん等がある。

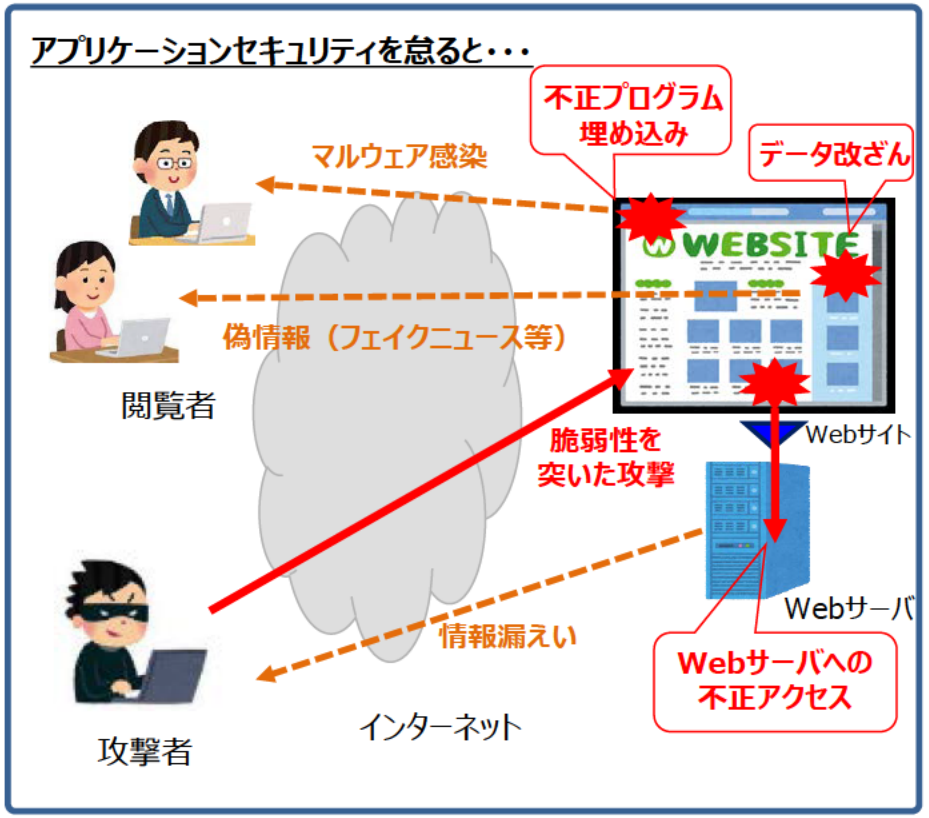
● Application Securityを怠ると？

– 最近のアプリケーションはネットワーク上で利用可能なものが多く、ネットワーク経由の脅威に晒されている状況。

– 特に、**Webアプリケーション**（Webサイト等）については、インターネット上での利用が前提であるため、攻撃者の標的になりやすく、セキュリティ事案も日常的に発生している状況。

✓ 2021年以降、日本において国際会議・世界大会が続いていく。

✓ 日本のWebサイトは大小問わずハクティビストや愉快犯の主張や攻撃力を誇示する場となりやすく、特に警戒が必要。



要対応項目４：アプリケーションの適切な管理（Application Security）２

● Webアプリケーションにおける主な対策方法は？

– Webアプリケーション開発の設計段階から、「脆弱性を作り込まない実装」を実現することが理想。

✓ 具体的には、それぞれの脆弱性の原因そのものをなくす根本的な解決策を講じることで、その脆弱性を狙った攻撃を無効化する。

– Webアプリケーションを格納するWebサーバのセキュリティ対策も考慮する必要がある。

✓ 具体的には、OSやソフトウェアの脆弱性対応、リモート操作する際の認証機能強化など。

– 運用段階では、脆弱性診断テスト（Webアプリケーションに内在する脆弱性を、ツールや手動診断により検出する）が有効。疑似攻撃（ペネトレーションテスト）を行うこともある。

✓ Webアプリケーションの脆弱性を利用した攻撃には、

- SQLインジェクション

  →DB不正操作による情報漏えい、データ改ざん

- クロスサイト・スクリプティング

  →不正サイト誘導によるマルウェア感染

などがある。

✓ いずれもよく知られた脅威であり、**基本的な対策で回避できる**ため、対策は必須。

【参考】安全なウェブサイトの作り方（IPA）

「安全なウェブサイトの作り方」は、IPAが届出を受けた脆弱性関連情報を基に作成した、ウェブサイト開発者や運営者が適切なセキュリティを考慮したウェブサイトを作成するための資料。

目次

https://www.ipa.go.jp/security/vuln/websecurity.html


METI
Ministry of Economy, Trade and Industry