個人情報保護法の改正への備え

（ソース：https://xtech.nikkei.com/atcl/nxt/column/18/00989/080500032/ ）

❖ 不正アクセスで漏洩なら1件でも本人に通知、法改正で増す個人情報保護の「重し」

❑ 企業の負担
- ✓ 情報漏洩被害者への詳細な報告・通知
- ✓ 監督官庁への詳細な報告
- ✓ 罰金
- ✓ 被害者へのお見舞金
- ※ 詳細な報告をするには、調査費用が発生

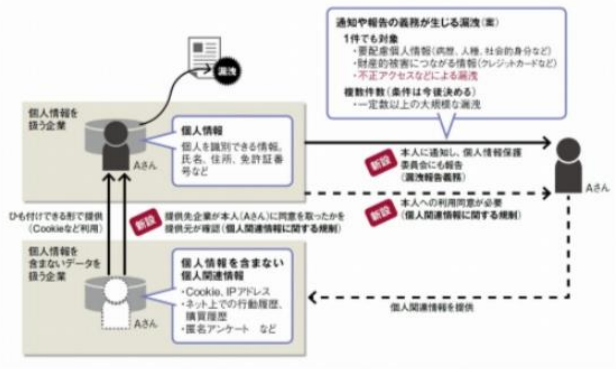
❑ 時期：2022年春以降に施行予定

想定される攻撃

- ✓ 不正アクセス（脆弱性）
- ✓ フィッシング
- ✓ ランサムウェア
- ✓ ネットワーク攻撃　など

公表控えは許されない

最も影響が大きいのが不正アクセスによる個人情報漏洩である。2020年6月の改正法成立を受け、政府が2020年7月に示した法運用の基本方針案によると、サイバー攻撃などの不正アクセスによる漏洩は、件数を問わず被害に遭った本人に通知するよう義務付けたからだ。同時に個人情報保護委員会への報告も義務化する。



改正個人情報保護法で新設する「漏洩報告義務」と「個人関連情報に関する規制」の概要

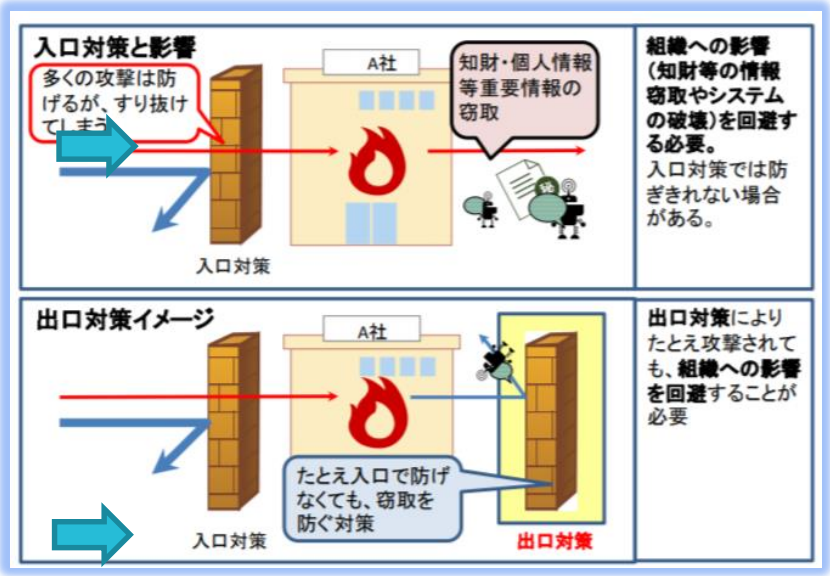
［画像のクリックで拡大表示］

IPA「脅威と対策研究会」による考察

【IPA「脅威と対策研究会」による考察】

新しい攻撃(標的型攻撃)への備え

- ✓ 従来の攻撃を防ぐ為の入口対策(●)
  - ➢ 不正アクセス
  - ➢ マルウェア感染
  - ➢ ネットワー攻撃
- ✓ たとえ組織の中に攻撃の一部が入り込まれたとしても、共通攻撃手法部分を止め、外部にいる攻撃者に情報を窃取されないための出口対策（■）
  - ➢ マルウェア感染
  - ➢ ボットネット　など



https://www.ipa.go.jp/files/000017308.pdf

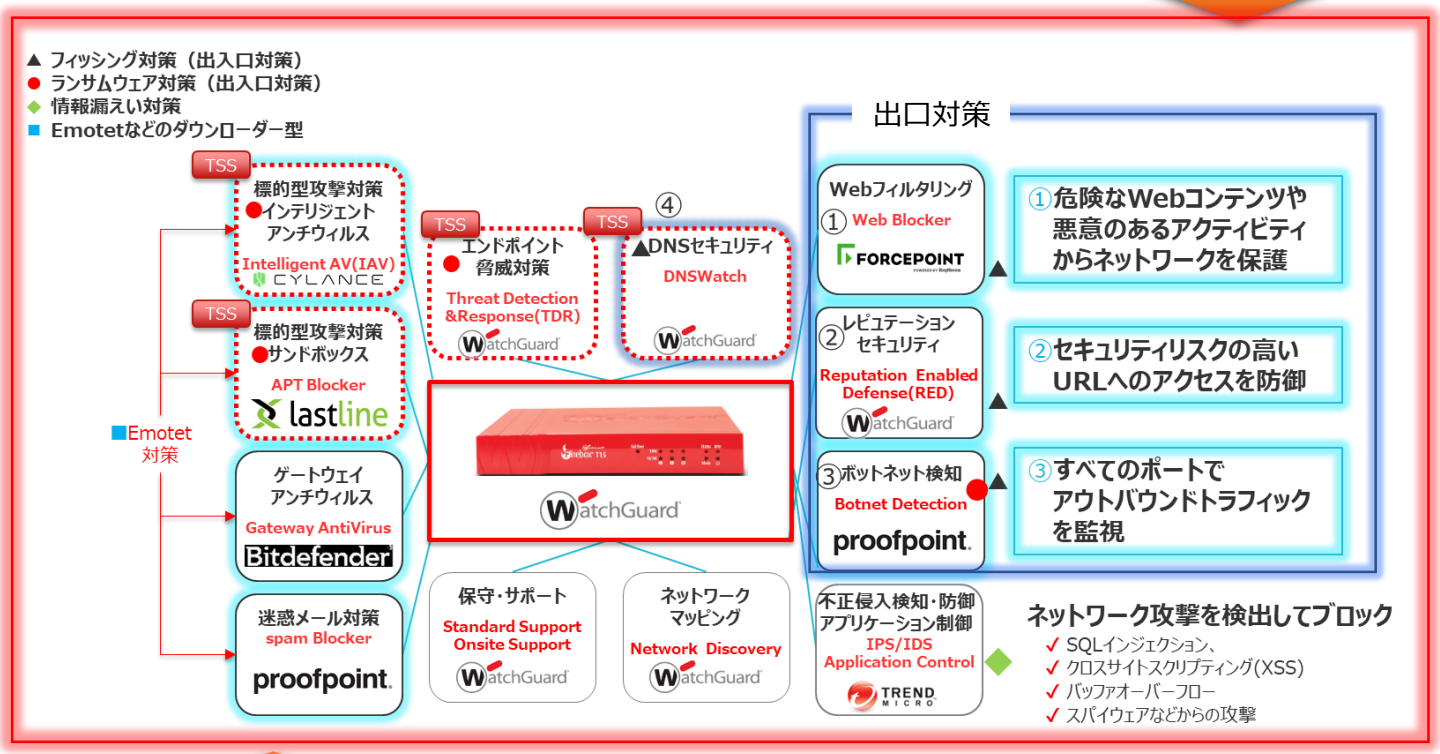
ウォッチガードによるフィッシング、ランサムウェア対策（出入口対策）

（ソース： https://www.antiphishing.jp/report/consumer_antiphishing_guideline_2020.pdf ）

3. 今すぐできるフィッシング対策 5
3.1. 正しい URL にアクセスする 5
3.1.1 正しいドメイン名を確認し、ブックマークに登録する 5
3.1.2 電子メール中のリンクはクリックしない 5
3.1.3 本来の Web サイトであるかどうかを確認する 7
3.1.4 モバイル端末向けの注意事項 8

フィッシングへの必要な備え

Firebox による対策



Fireboxによる対策

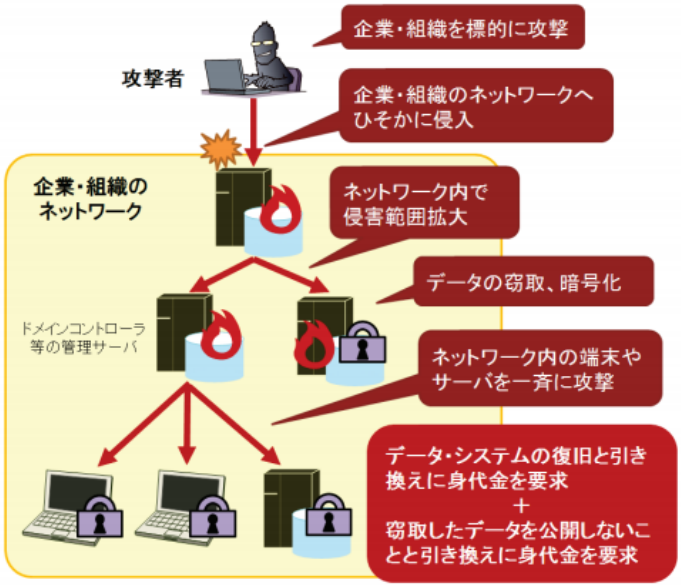
企業・組織のネットワークへの侵入対策

- この攻撃は、攻撃者が企業・組織のネットワークへ侵入するところから始まります。
- 特に、インターネットからアクセス可能な状態としているサーバへの不正アクセスや、ネットワーク機器の脆弱性の悪用などが報告されています。
- リモートデスクトップサービス（RDP）の認証を突破されたり、VPN装置のアップデートが行われておらず侵入されたという事例が多くありますが、狙われるのはこれらに限りません。
- インターネットからアクセス可能な装置全体について、アクセス制御が適切にできているか、認証が突破される可能性はないか、脆弱性は解消されているかといった点を、今一度確認することを勧めます。

加えて、データ・システムのバックアップが必要です

ソース：
https://www.ipa.go.jp/security/announce/2020-ransom.html

新たなランサムウェア攻撃



ソース： https://www.ipa.go.jp/files/000084974.pdf