

サイバー攻撃の傾向と対策



**奈良工業高等専門学校 情報工学科
サイバーセキュリティ教育研究部門
(併)大阪大学 大学院情報科学研究科**

岡村 真吾

自己紹介

岡村 真吾 博士(情報科学)(大阪大学)

• 略歴

- 1998.3 大阪府立高専 電子情報工学科 卒業
- 2000.3 大阪大学 基礎工学部 情報科学科 卒業
- 2005.3 大阪大学 大学院情報科学研究科
博士後期課程修了 博士(情報科学)
- 2005.4 大阪大学 サイバーメディアセンター
- 2008.4 大阪大学 大学院情報科学研究科
- 2008.10 奈良高専 情報工学科

• 研究分野

サイバーセキュリティ(プライバシー保護、コンテンツ保護、
認証・認可、暗号プロトコルなど)

情報セキュリティ10大脅威 2021（組織）



昨年

1	ランサムウェアによる被害	5
2	標的型攻撃による機密情報の窃取	1
3	テレワーク等のニューノーマルな働き方を狙った攻撃	New
4	サプライチェーンの弱点を悪用した攻撃	4
5	ビジネスメール詐欺による金銭被害	3
6	内部不正による情報漏えい	2
7	予期せぬIT基盤の障害に伴う業務停止	6
8	インターネット上のサービスへの不正ログイン	16
9	不注意による情報漏えい等の被害	7
10	脆弱性対策情報の公開に伴う悪用増加	14

IPA「情報セキュリティ10大脅威 2021」<https://www.ipa.go.jp/security/vuln/10threats2021.html>

サイバー攻撃・事故の傾向

- **対象を定めた攻撃**
 - 標的型攻撃による機密情報の窃取
 - ビジネスメール詐欺による金銭被害
 - ランサムウェアによる被害
- **内部からの情報漏えい**
 - 内部不正による情報漏えい
 - 不注意による情報漏えい等の被害
- **テレワークやクラウドサービスの利用に関する事故**
 - テレワーク等のニューノーマルな働き方を狙った攻撃
 - 予期せぬIT基盤の障害に伴う業務停止
 - インターネット上のサービスへの不正ログイン

対策の基本的な考え方

- **フェーズ**
 - 予防
 - 事故が起こらないようにする（アクセス制限など）
 - 事故が起こったときの被害を抑える（暗号化など）
 - 事後対応
 - 被害の拡大を防ぐ（不審な通信の検知など）
- **手段**
 - 技術の導入
 - ルールや手順、体制の整備
 - 教育の実施

標的型攻撃

- **特定の組織を狙って、機密情報等を得ようとする。**
- **手段**
 - **メールの添付ファイルやリンク先を開かせることでマルウェアに感染させる。**
 - **組織でよく利用されるウェブサイトを改ざんし、そこからマルウェアに感染させる。**
 - **組織が利用するクラウドサービス等を攻撃して、認証情報を得る。**
- **結果**
 - **攻撃者が組織内部への侵入に成功する。**
 - **組織内部を探索し、機密情報を得る。**

ビジネスメール詐欺

- **取引先等を装って偽のメールを攻撃対象の組織へ送り、攻撃者の口座へ送金させる。**
 - 偽の請求書を送る
 - 「口座が変わった」
- **メール送信元のアドレスを偽装している、もしくは乗っ取られている。**
- **攻撃者は正規のやりとりの情報を入力している？**

標的型攻撃対策

- **ユーザ教育**
 - 添付ファイルを安易に開かない、開き方のルールを決める
 - リンク先を確認する(表示されている文字列ではなく)
- **権限の制限**
 - 実行できる機能を制限する
- **検知**
 - セキュリティ対策ソフト
 - ネットワーク監視
 - メール発信元の確認(送信ドメイン認証など)
 - 電話等の別手段での確認

ランサムウェア

- Ransomware
- **ファイルを暗号化し身代金(ransom)を要求する**
 - お金を支払えば、復号できるかも知れないし、できないかも知れない
- **暴露型ランサムウェア**
 - 被害者の手元のファイルを暗号化すると共に、ファイルを攻撃者へアップロードする
 - お金を支払わなければ、攻撃者の手元にあるファイルを公開される

ランサムウェア対策

- **ファイルのバックアップを取っておく**
 - 暗号化された場合は、バックアップから復元する
 - 日頃から、バックアップが復元できるかを確認しておく
- **ファイルを暗号化して保存しておく**
 - 攻撃者へアップロードされても閲覧を困難にする

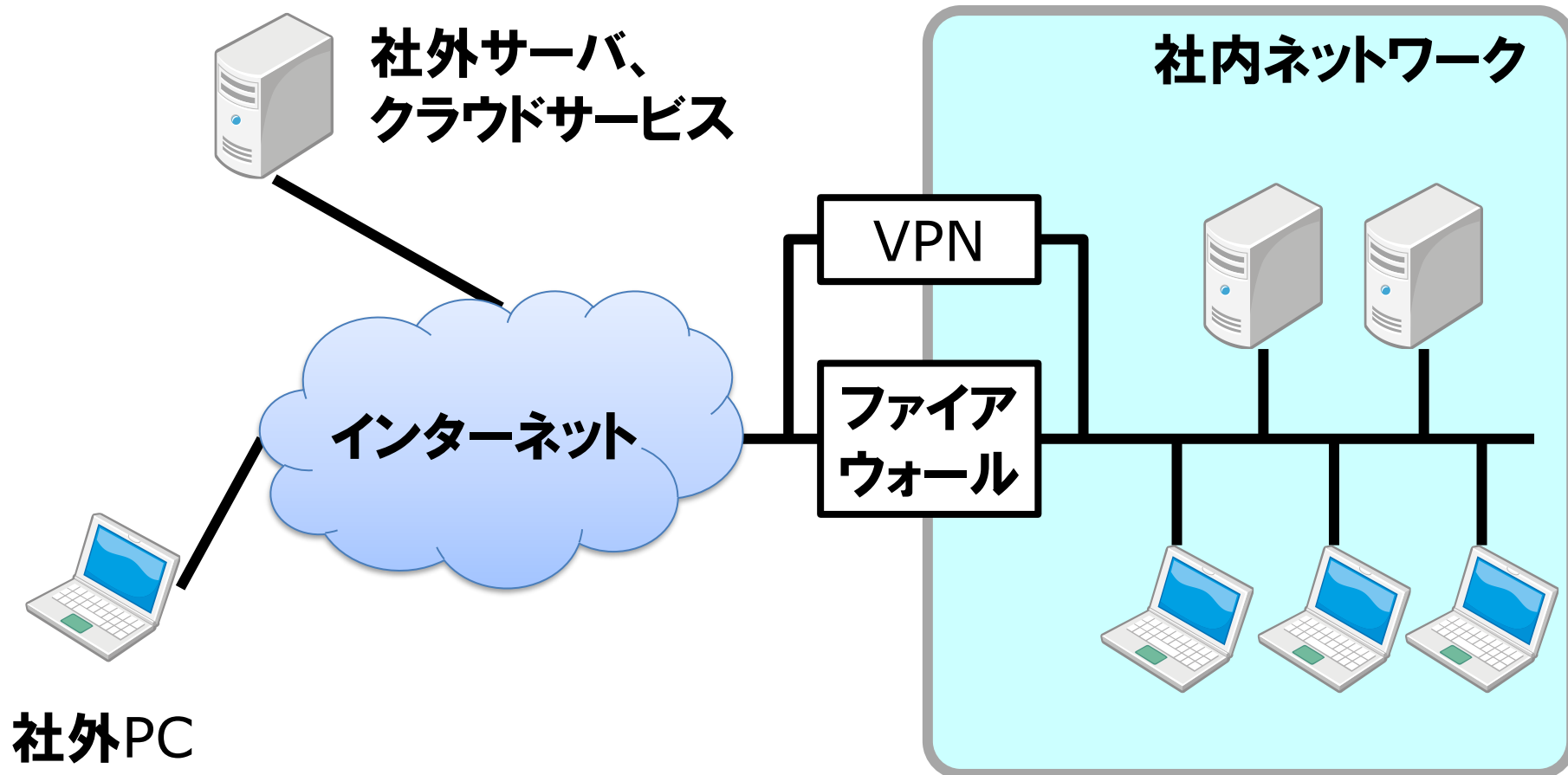
内部からの情報漏えい

- **不注意による情報漏えい等の被害**
 - メールの誤送信(宛先間違い、添付間違いなど)
 - ウェブサーバへのアップロード
 - PCやUSBメモリ等の紛失
 - 画像やPDFの加工ミス
- **内部不正による情報漏えい**
 - (元)従業員による機密情報の持ち出し
 - 競合他社への情報提供

情報漏えい対策

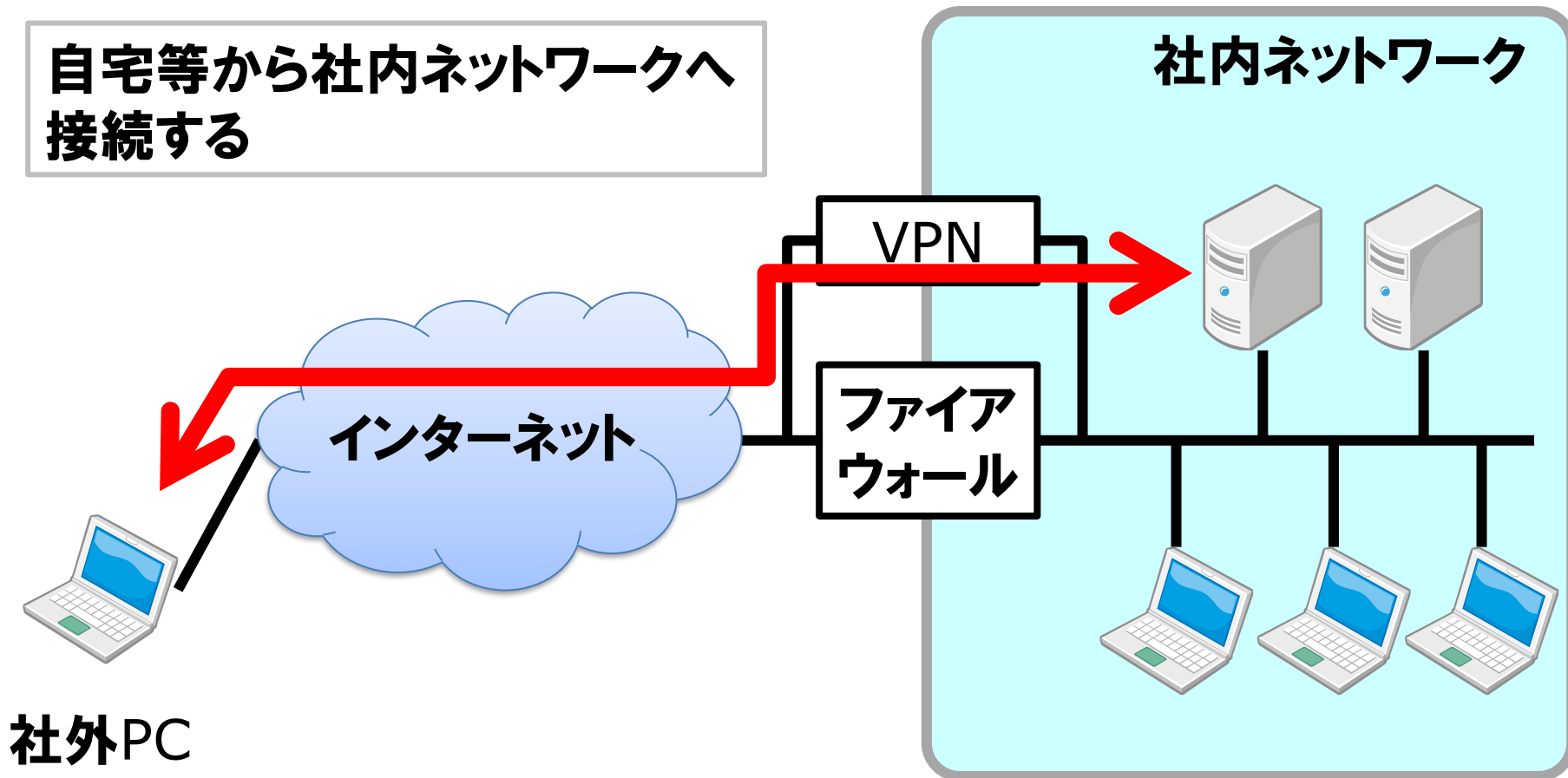
- **ルール、手順を決める**
 - 機密性のレベルによって保管場所を変える
 - ファイル生成時にパスワードを付与
 - 加工(墨消し)方法
 - メール送信時やアップロード時の確認手順
 - 持ち出す情報は最小限に
 - 担当者が変わったときに権限・パスワードを変更
- **複数人で扱う**
 - 重要な情報を扱う場合は複数人が関わる仕組み作り
 - アクセス履歴の記録と定期的な監査

テレワーク

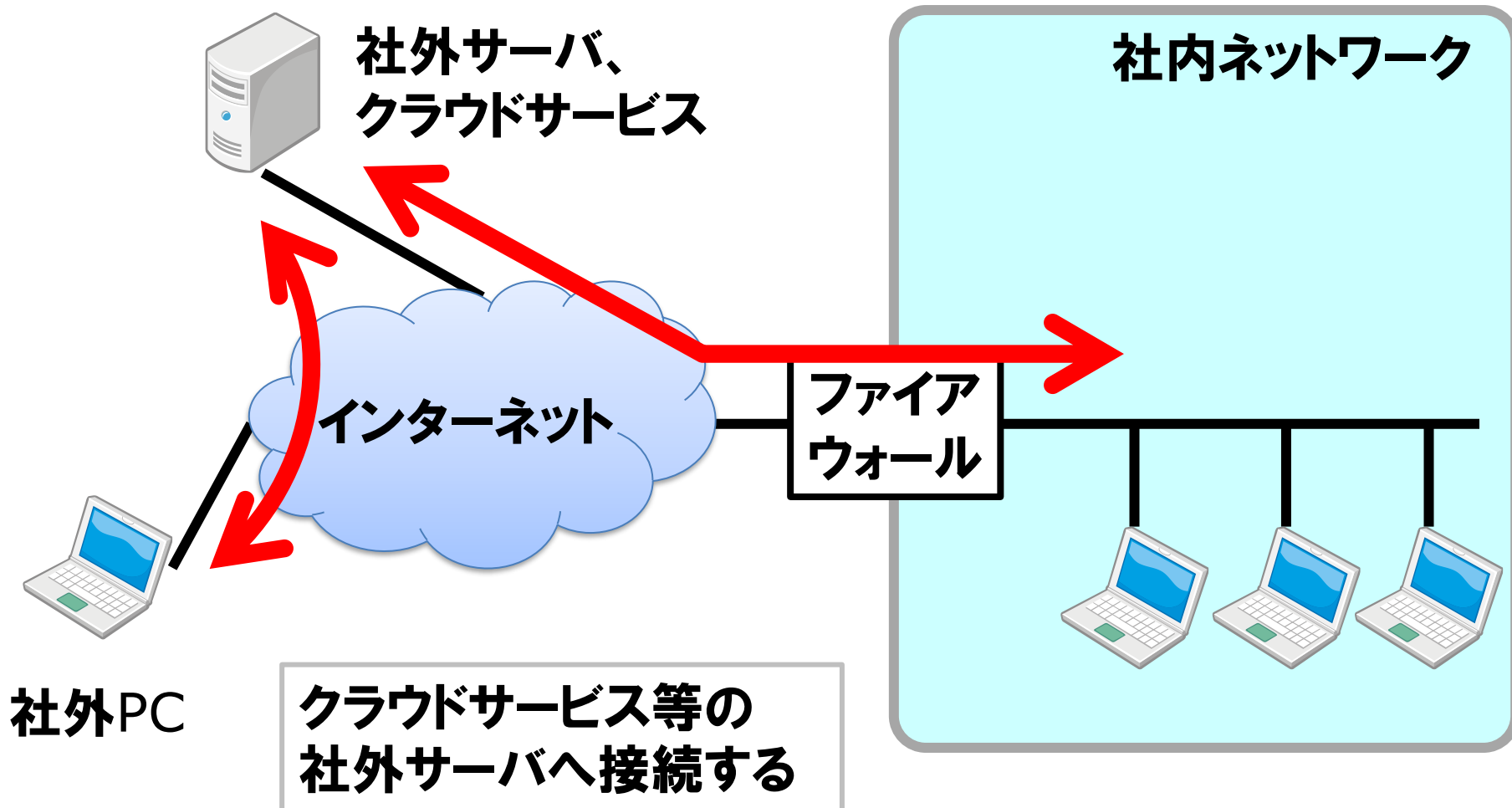


VPN、リモートデスクトップを利用

自宅等から社内ネットワークへ
接続する



クラウドサービスを利用



テレワークの脅威

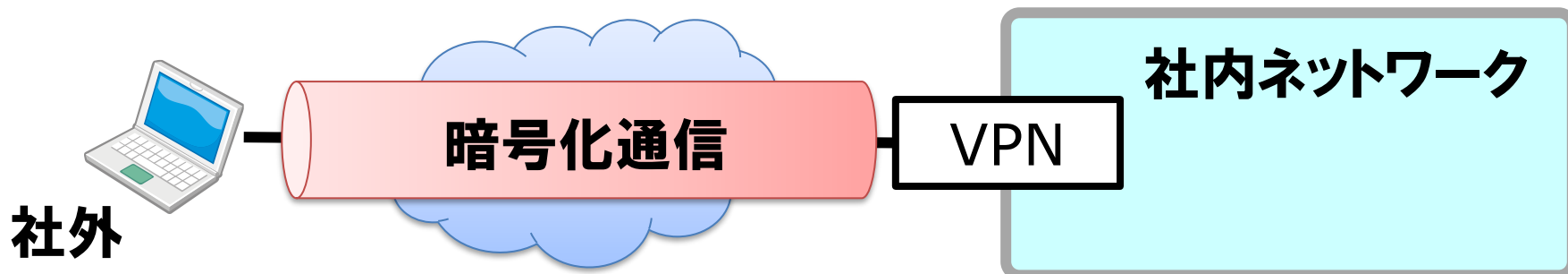
- **攻撃手法**
 - マルウェア(不正プログラム)感染
 - 添付ファイル、リンク
 - 不正アクセス
 - パスワード攻撃、脆弱性の利用
 - 端末の紛失・盗難
 - 盗聴
- **結果**
 - 情報漏えい
 - 業務停止
 - 信用失墜

情報や機器の持ち出しへの対策

- **情報の格付け**
 - 機密性、完全性、可用性
- **情報セキュリティポリシー、マニュアル**
 - 格付けに応じた取り扱いを定める
- **事故発生時の対応手順**
- **利用者教育**

VPN

- Virtual Private Network
- インターネット等の社外ネットワークを経由して、社内ネットワーク内のサーバ等を利用する
- 社内ネットワークとの間で暗号化通信を行い、社外のPCを社内ネットワークに属しているように扱う
- 基本的な考え方は「内は安全、外は危険」
→ **不正アクセスされて内部に侵入されると脆弱**

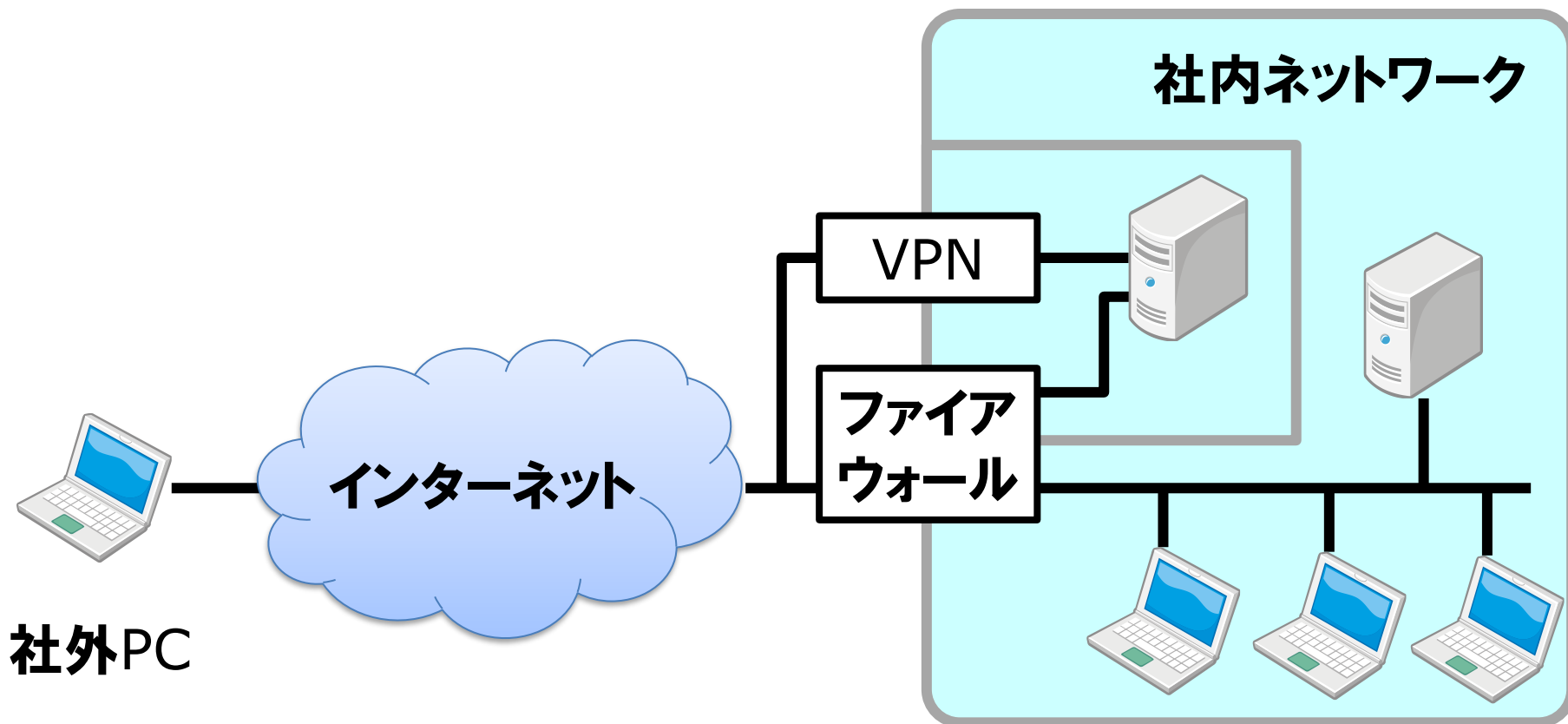


VPNの選び方とセキュリティ強化

- Selecting and Hardening Remote Access VPN Solutions
- **アメリカの国家安全保障局(NSA)と国土安全保障省サイバーセキュリティインフラセキュリティ庁(CISA)が2021年9月28日に発表**
- **次のことを推奨**
 - **標準的な技術(IKE/IPsecなど)を用いた製品を使用する**
 - **検証を受けた製品を使用する**
 - **公開鍵による認証もしくは多要素認証を用いる**
 - **アクセス先や利用できる機能を必要最小限に制限する**
 - **セキュリティアップデートを適用する**
 - **ログを記録し、監視する**

アクセス先の制限

社内ネットワークのうち、外部からもアクセス可能なものと内部からのみアクセス可能なものに分ける



テレワークで使用する端末

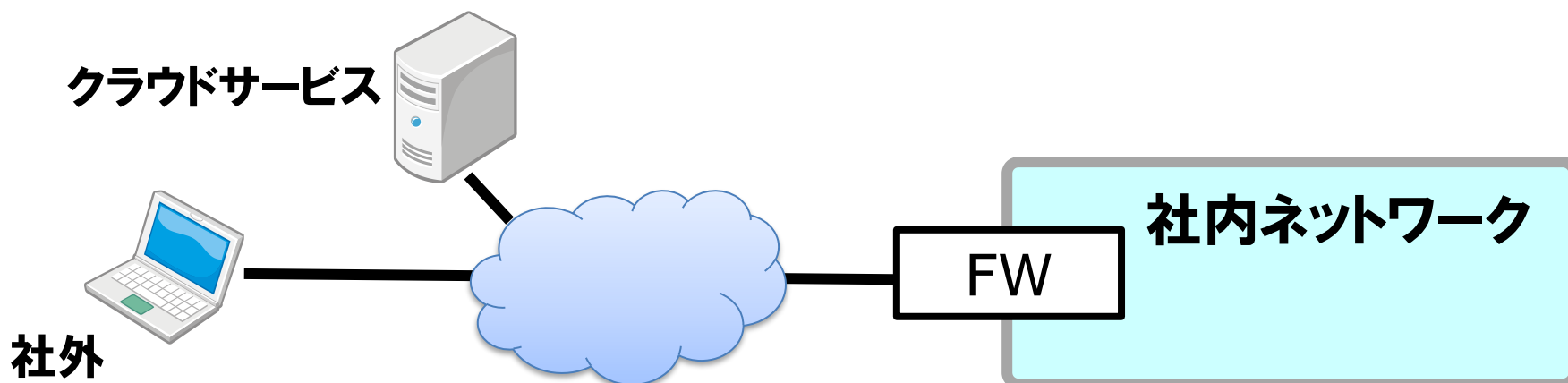
- **会社から支給**
 - **基本**
- **個人所有(本人が占有)**
 - **本人に技術や知識があるなら・・・**
- **個人所有(家族で共有)**
 - **本人が余程の玄人でない限りやめた方がよい**
会社は家族をコントロールできない

ゼロトラストセキュリティ

- Zero Trust Security
 - 内と外を区別しない(内部であっても信用しない)
 - アクセスしてくるものを無条件に信用しない
- 内部からであってもアクセスしてくるものをしっかりと検証(認証)する

クラウドサービスの注意点

- システム停止、ネットワーク停止
 - 一時的にサービスが利用不可になる
 - 数時間から数日に渡る場合も
- データの消失
 - バックアップを取っておく
- データセンターが設置されている場所(国)
 - その国のルールが適用される



インターネット上のサービスへの不正ログイン

- **パスワード認証に対する攻撃**
 - **総当たり(ブルートフォース)攻撃**
 - IDを固定してパスワードとしてあり得るパターンを全て試す
 - **リバースブルートフォース攻撃**
 - パスワードを固定してIDとしてあり得るパターンを全て試す
 - **辞書攻撃**
 - パスワードとしてよく用いられるパターン(辞書)を試す
 - **パスワードリスト攻撃**
 - 別のサイトから入手したIDとパスワードの組を試す

不正ログイン対策

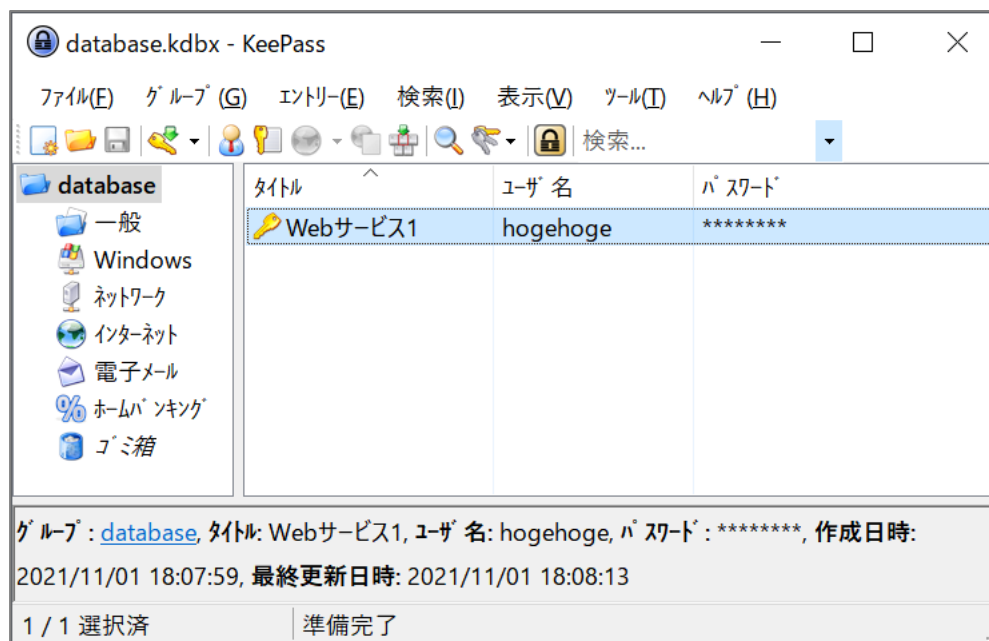
- **パスワード認証をやめる**
 - **多要素認証**
- **複数のサービスで同じパスワードを使い回さない**
- **覚えられるパスワードは使わない**
 - **パスワード管理ツールを使う**

多要素認証

- **複数の要素を組み合わせてユーザを認証する。**
 - **要素**
 - **本人の知識**
 - 暗証番号、パスワードなど
 - **本人の所有物**
 - 鍵、カードなど
 - **本人の特徴**
 - 声、顔、静脈、虹彩など
- **パスワード入力 + スマートフォンのアプリ など**

パスワード管理ツール

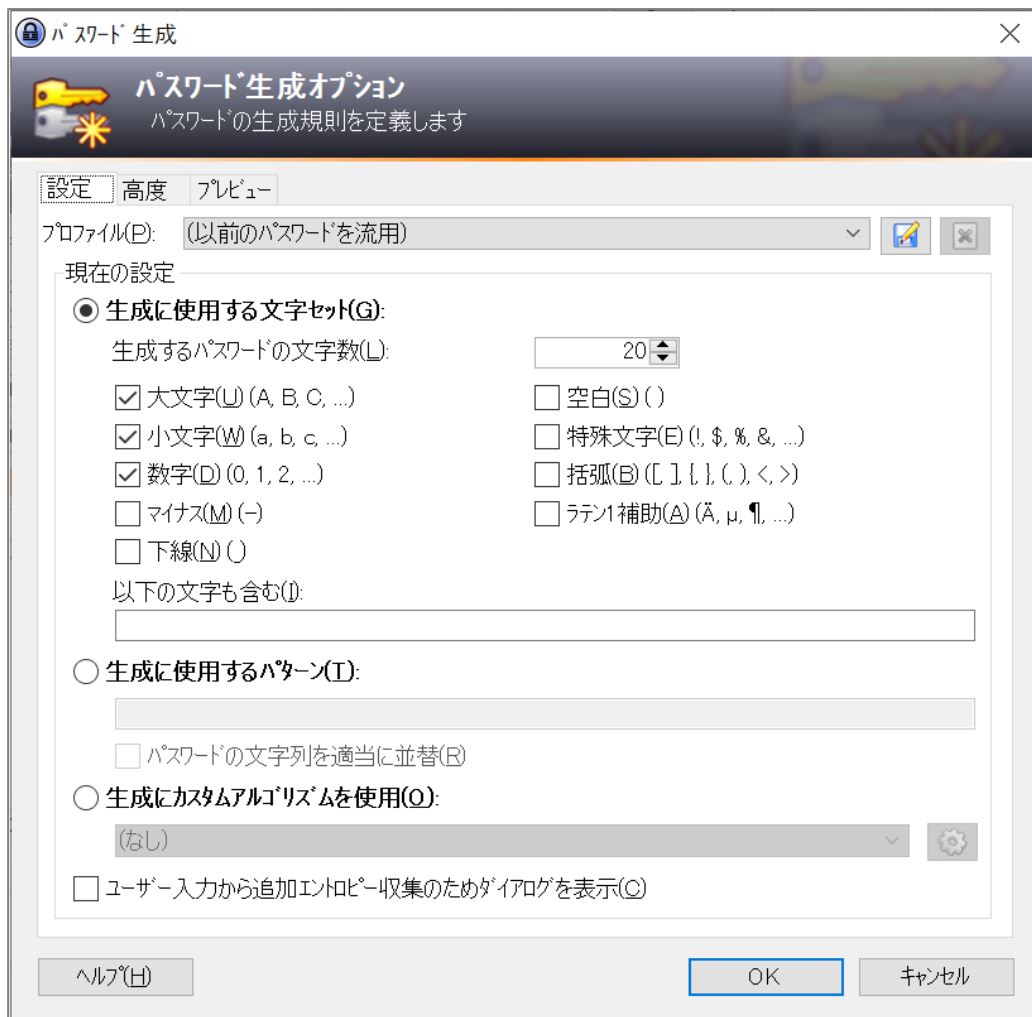
- パスワードの生成
- パスワードの保存



ツール例: KeePass

KeePass Password Safe, <https://keepass.info/>

パスワードの生成



← 文字数や使用する文字の種類を指定

KeePass Password Safe, <https://keepass.info/>

参考情報

- 国民のための情報セキュリティサイト(総務省)
- 中小企業の情報セキュリティ対策ガイドライン(IPA)
- インターネットの安全・安心ハンドブック(NISC)

国民のための情報セキュリティサイト

- https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/
- **基礎知識、一般利用者の対策、企業・組織の対策**



The screenshot shows the homepage of the National Information Security Site. At the top, there is a search bar and a navigation menu. The main heading is "国民のための情報セキュリティサイト" (Information Security Site for the People). Below the heading, there is a paragraph of text: "正しい知識と対策によって、安心して便利なインターネットを活用しましょう。このホームページでは、インターネットと情報セキュリティの知識の習得に役立ち、利用方法に応じた情報セキュリティ対策を講じるための基本となる情報をご提供します。" (By using correct knowledge and countermeasures, you can safely and conveniently use the Internet. On this homepage, we provide information that is helpful for acquiring knowledge of the Internet and information security, and basic information for implementing information security countermeasures according to the method of use.)

There are several sections on the page:

- トピックス (Topics):** A yellow box containing two items:
 - > 「Wi-Fi利用者向け 簡易マニュアル(令和2年5月版)」を公開しました。(2020/5/29)
 - > 「Wi-Fi提供者向け セキュリティ対策の手引き(令和2年5月版)」を公開しました。(2020/5/29)
- はじめに (Introduction):** A section with a question mark icon, containing three links:
 - スマートフォン 情報セキュリティ3か条 (Smartphone Information Security 3 Principles)
 - 情報セキュリティ初心者 のための三原則 (Three Principles for Information Security Beginners)
 - Wi-Fi (無線LAN) の安全な利用について (About Safe Use of Wi-Fi)
- 基礎知識 (Basic Knowledge):** A section with a magnifying glass icon.
- 一般利用者の対策 (Countermeasures for General Users):** A section with a person icon.
- 企業・組織の対策 (Countermeasures for Companies/Organizations):** A section with a person icon.

中小企業の情報セキュリティ対策ガイドライン

- IPA(独立行政法人情報処理推進機構)が発行
- <https://www.ipa.go.jp/security/keihatsu/sme/guideline/>

ガイドライン等のダウンロード



(本編)

- 本編：中小企業の情報セキュリティ対策ガイドライン第3版（全60ページ、32.56MB）
- 付録1：情報セキュリティ5か条（全2ページ、726KB）
- 付録2：情報セキュリティ基本方針（サンプル）（全1ページ、35KB）
- 付録3：5分でできる！情報セキュリティ自社診断（全8ページ、3.9MB）
- 付録4：情報セキュリティハンドブック（ひな形）（全11ページ、212KB）
- 付録5：情報セキュリティ関連規程（サンプル）（全51ページ、179KB）
- 付録6：クラウドサービス安全利用の手引き（全8ページ、2.8MB）
- 付録7：リスク分析シート（全7シート、99KB）



(付録1)



(付録3)



(付録6)

インターネットの安全・安心ハンドブック

- 内閣サイバーセキュリティセンターが発行
- <https://www.nisc.go.jp/security-site/handbook/>



The screenshot shows the NISC (National Institute of Cyber Security) website. At the top left is the NISC logo and name in Japanese and English. Below it is a navigation menu with links for 'TOP', '初心者の方へ' (For beginners), 'スマートフォン利用者の方へ' (For smartphone users), '家庭で' (At home), '学校で' (At school), and '会社で' (At work). Underneath are more specific links: 'サイバーセキュリティ月間' (Cyber Security Month), 'サイバーセキュリティ国際キャンペーン' (International Cyber Security Campaign), '困ったときに' (When in trouble), 'テレワーク実施者の方へ' (For teleworkers), and 'パソコンを使い始める小中学生のみなさんへ' (For elementary and middle school students starting to use PCs).

The main content area features a large yellow banner with the text: 'セキュリティが分からなければこの1冊' (If you don't know security, this is the only book you need), 'インターネットの' (Internet's), and '安全・安心ハンドブック' (Safety and安心 Handbook). To the right of the banner is a small image of the handbook cover, which includes the text 'インターネットの 安全・安心 ハンドブック' and 'NISC'.

Below the banner, there is a breadcrumb trail: 'TOP | インターネットの安全・安心ハンドブック'. On the left, there is a link: '「インターネットの安全・安心ハンドブック」について' (About the Internet Safety and安心 Handbook). On the right, there are three blue buttons: '初心者の方へ' (For beginners), 'スマートフォン利用者の方へ' (For smartphone users), and '家庭で' (At home).

まとめ

• 傾向

- 対象を定めた攻撃
 - 標的型攻撃、ビジネスメール詐欺、ランサムウェア
- 内部からの情報漏えい
 - 内部不正、不注意
- テレワークやクラウドサービスの利用に関する事故
 - VPN、IT基盤の障害、不正ログイン

• 対策

- 技術の導入
- ルールや手順、体制の整備
- 教育の実施

本内容についてのお問い合わせ先

岡村 真吾

(奈良工業高等専門学校 情報工学科)

okamura@info.nara-k.ac.jp

<https://www.info.nara-k.ac.jp/security/>